НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет Інформатики та обчислювальної техніки

Обчислювальної техніки

До захисту допущено:

Завідувач кафедри

_____ Сергій Стіренко

«___»_____2020 р.

Дипломний проєкт

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Комп'ютерні системи та мережі»

спеціальності 123 «Комп'ютерна інженерія»

на тему: «Метод захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах та програмні засоби його реалізації»

Виконав: студент 4 курсу, групи ІО-61
Іасешвілі Георгій Нугзарович _____
(підпис)

Керівник:
доц. к.т.н. Марковський Олександр Петрович _____
(підпис)

Консультант з нормо-контролю:
проф. д.т.н. Сімоненко Валерій Павлович _____
(підпис)

Рецензент: _____
(підпис)

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Факультет Інформатики та обчислювальної техніки

Обчислювальної техніки

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Сергій Стіренко
«___»_____2020 р.

ЗАВДАННЯ

на дипломний проєкт студенту

Іасешвілі Георгія Нугзаровича

1. Тема проєкту «Метод захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах та програмні засоби його реалізації», керівник проєкту Марковський Олександр Петрович, доц., к.т.н., затверджені наказом по університету від «07» травня 2020 р. № 1081-с

2. Термін подання студентом проєкту _____

3. Вихідні дані до проєкту

4. Зміст пояснювальної записки

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо)

6. Консультанти розділів проєкту

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормо-контроль	Сімоненко В. П. проф.		

7. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1.	Затвердження теми роботи	01.09.2019	
2.	Вивчення та аналіз завдання		
3.	Розробка архітектури та загальної структури систем		
4.	Розробка структур окремих підсистем		
5.	Програмна реалізація системи		
6.	Оформлення пояснювальної записки		
7.	Захист програмного продукту		
8.	Передзахист	26.05.2020	
9.	Захист		

Студент Георгій Іасешвілі

Керівник Олександр Марковський

ОПИС АЛЬБОМУ

№ з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
1	А4	ІАЛЦ.468243.002	Технічне завдання	3	
2	А4	ІАЛЦ.468243.003 ПЗ	Метод захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах та програмні засоби його реалізації		
3			Пояснювальна записка	72	
4	А4	ІАЛЦ.468243.004	Функціональна схема	1	
5	А4	ІАЛЦ.468243.005	Принципова схема	1	
6	А4	ІАЛЦ.468243.006	Структурна схема	1	
7	А4	ІАЛЦ.468243.007	Лістинг програми	3	
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21					
22					
23					
24					
25					
26					
27					

Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Іасешвілі Г.Н.			*Метод захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах та програмні засоби його реалізації* Відомість дипломного проєкту	Літ.	Арк. 1 / Акрушів
Перевір.		Марковський О.П.					КПІ ім. Ігоря Сікорського ФІОТ ІО-61
Н. Контр.		Сімоненко В.П.					
Затверд.		Стіренко С.Г.					

28					

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Іасешвілі Г.Н.			*Метод захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах та програмні засоби його реалізації* Відомість дипломного проєкту	Літ.	Арк.	Акрушів
Перевір.		Марковський О.П.					1	
						КПІ ім. Ігоря Сікорського ФІОТ ІО-61		
Н. Контр.		Сімоненко В.П.						
Затверд.		Стіренко С.Г.						

ТЕХНІЧНЕ ЗАВДАННЯ

ЗМІСТ

1. НАЙМЕНУВАННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ

Технічне завдання поширюється на методу захищеної реалізації перетворень Фур’є на віддалених комп’ютерних системах та програмних засобів його реалізації.

Область застосування – віддалені комп’ютерні системи великої потужності та хмарні технології надання їх обчислювальних ресурсів користувачам.

2. ПІДСТАВИ ДЛЯ РОЗРОБКИ

Підставою для розробки є завдання на виконання роботи кваліфікаційно-освітнього рівня “бакалавр комп’ютерної інженерії”, затверджене кафедрою спеціалізованих комп’ютерних систем Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”.

3. МЕТА ТА ПРИЗНАЧЕННЯ РОЗРОБКИ

Мета проекту полягає в організації захисту даних користувачів в процесі виконання над цими даними прямого та зворотного перетворень Фур'є на віддалених комп’ютерних системах за рахунок застосування нового методу гомоморфного шифрування даних перед їх передачею на віддалену обробку.

Розробка призначена для прискорення реалізації важливої операції цифрової обробки сигналів - дискретного перетворення Фур'є за рахунок безпечного в інформаційному плані залучення обчислювальних потужностей віддалених багатопроцесорних комп’ютерних систем з використанням хмарних технологій.

4. ДЖЕРЕЛА РОЗРОБКИ

4.1 Markovskyi O.P. Secure Modular Exponentiation in Cloud Systems/ O.P. Markovskyi, N. Bardis, S.J. Kirilenko // Proceeding of the Congress on Information Technology. Computationnal and Experimental Physics (CITCEP 2015), 18-20 December 2015, Krakow. Poland. – PP.266-269.

4.2 Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – Issue 4. – 2012. – №3. – PP. 169-180.

4.3 Марковський О.П. Захищена реалізація фільтрації зображень в GRID-системах / О.П. Марковський, М.В. Невдащенко, А.М. Білашевська // Вісник Національного технічного університету України ”КПІ” Інформатика, управління та обчислювальна техніка. – Київ: ВЕК+. – 2014. – № 61. – С.105-109.

4.4 Буйбарова М.Ф. Метод захищеної реалізації перетворень Фур’є на віддалених розподілених комп’ютерних системах / М.Ф. Буйбарова, Ю.М. Виноградов, В.Ю. Приймак // Вісник Національного технічного університету України “КПІ” Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+”. – № 64. – 2016. – С. 64-71.

5. ТЕХНІЧНІ ВИМОГИ

5.1. Вимоги до продукту, що розробляється

5.1.1 Для гомоморфного шифрування даних користувачів перед їх віддаленим виконанням над ними дискретного перетворення Фур'є використовувати методи на основі адитивного та ланцюжкового накладання секретних ключів.

5.1.2 Гомоморфне шифрування даних користувачів перед їх віддаленим виконанням над ними дискретного перетворення Фур'є має використовувати

прості процедури шифрування та дешифрування, так, щоб питома вага обчислень, які виконуються користувачем на його обчислювальній платформі становила не більше 8% від загального об’єму обчислень, пов’язаних з реалізацією дискретного перетворення Фур'є.

5.1.3 Довжина ключа гомоморфного шифрування відліків сигналів при їх віддаленого перетворенню Фур'є має біти не меншою від 128 бітів.

5.1.4 Розрядність відліків сигналу для захищеної віддаленої обробки на комп’ютерних системах – 64 в форматі з плаваючою точкою.

5.1.5 Кількість відліків сигналу користувача, що передається для виконання перетворення Фурє на віддалених комп’ютерних системах – до 128.

5.2. Вимоги до програмного забезпечення

- Операційна система MS Windows 10
- Visual Studio 2017
- C++11

5.3. Вимоги до апаратної частини

- Процесор рівня Intel i5 і вище.
- Оперативна пам’ять не менше 500 МБ.
- Вільне місце на жорсткому диску не менше 100 МБ.

6. ЕТАПИ РОЗРОБКИ

	Дата
Вивчення літератури	20.12.2019
Створення та узгодження технічного завдання	15.01.2020
Вивчення літературних джерел	27.01.2020
Розробка алгоритму гомоморфного шифрування	15.04.2020
Розробка програмної моделі	01.05.2020
Відлагодження програми та виправлення помилок	15.05.2020
Оформлення документації дипломного проекту	06.06.2020

Пояснювальна записка
до дипломного проєкту
на тему: «Метод захищеної реалізації перетворень Фур’є на віддалених комп’ютерних системах та програмні засоби його реалізації»

Київ – 2020 року

Змн.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Іасешвілі Г.Н.			*Метод захищеної реалізації перетворень Фур’є на віддалених комп’ютерних системах та програмні засоби його реалізації* Відомість дипломного проєкту	Літ.	Арк.	Акрушів
Перевір.		Марковський О.П.					1	
						КПІ ім. Ігоря Сікорського ФІОТ ІО-61		
Н. Контр.		Сімоненко В.П.						
Затверд.		Стіренко С.Г.						

Зміст

Змн.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Іасешвілі Г. Н.			*Метод захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах та програмні засоби його реалізації* Пояснювальна записка	Літ.	Арк. 2 / Акрушів
Перевір.		Марковський О.П.					
						КПІ ім. Ігоря Сікорського ФІОТ ІО-61	
Н. Контр.		Сімоненко В.П.					
Затверд.		Стіренко С.Г.					

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується високою динамікою розвитку інтерфейсу між зовнішнім світом та комп'ютерними системами обробки даних. Високими темпами вдосконалюються засоби сприйняття, вводу та розпізнавання зображень, відеоданих, мови. Середина другого десятиліття двохтисячних відзначилася високими темпами розвитку компактних та дешевих відео систем, засобів передачі даних, технологіями їх трансформації до зручного для обробки виду, методів їх розпізнавання на аналізу.

Важливе місце в цьому ланцюжці посідають технології актуалізації інформації про об'єкти зовнішнього світу та приведення її до зручного для обробки вигляду. Поняття актуалізації, або інформаційної фільтрації, включає в цьому контексті відсіювання всієї зайвої для подальшої обробки і прийняття рішень інформації [1]. Одною із найбільш поширених на практиці технологій інформаційної фільтрації та трансформації широкого кола сприйнятих приладами сигналів до зручного для подальшої обробки виду, є їх спектральне перетворення. Таке перетворення здійснюється через використання перетворення Фур'є. Це перетворення дозволяє приводити сигнали різної природи (зображення, голосі сигнали. сейсмограми, радіосигнали) до стандартного представлення у вигляді наборів дійсних чисел: кожна пара чисел вказує на амплітуду та фазу синусоїдального сигналу, на які може бути розкладений довільний сигнал. Це дає змогу порівнювати та аналізувати сигнали, здійснювати їх розпізнавання.

Висока ресурсоємність процедур швидкого перетворення Фур'є, визначається великою кількістю точок вимірів сигналу диктує практичну доцільність використання потужних багатопроцесорних віддалених комп'ютерних систем. Аналіз обчислювальних процедур швидкого перетворення Фур'є [2] показує, що вона допускає широке розпаралелювання,

що також педалює доцільність залучення віддалених багатопроцесорних потужних систем. Ще одним чинником на користь такої організації обробки сигналів з використання перетворень Фур'є є те, що дуже часто існують жорсткі часові обмеження на його реалізацію в практичних застосуваннях.

Серйозною перепоною на шляху широкого використання можливостей хмарних обчислень для реалізації перетворень Фур'є виступає характер обмежень доступу до сигналів та зображень. Саме це суттєвим чином обмежує їх обробку у відкритих системах, в тому числі GRID-системах. Відповідно, виникає практична потреба в організації захищеної реалізації перетворень Фур'є в сучасних відкритих розподілених комп'ютерних системах великої потужності [3] в рамках хмарних технологій. Основна вимога при організації захищеної реалізації перетворень Фур'є на віддалених і практично непідконтрольних обчислювальних потужностях полягає в тому, що воно має практично унеможливити доступ до оригінальних сигналів в процесі їх передачі і при обробці на віддаленій комп'ютерній системі.

Якщо захисти інформацію про сигнали користувача можна в процесі передачі, використовуючи симетричне чи потокове її шифрування, то захист такої інформації безпосередньо в процесі обробки становить складну проблему. Очевидно, що тип шифрування даних має залежати від обчислювальної процедури, яка здійснюється на віддаленій комп'ютерній системі. Такий тип шифрування даних отримав назву гомоморфного шифрування [4]. Це потребує розробки спеціальних шифрів, які гомоморфні обчисленням, які виконуються над даними.

Як уже зазначалося, однією із найбільш масових операцій обробки сигналів є дискретне перетворення Фур'є, яке широко використовується багатьох галузях науки, техніки та технологій. Зокрема в мобільному зв'язку широко використовується швидке перетворення Фур'є для декодування фази модуляції. Швидкий розвиток систем розпізнавання ситуацій, сцен, зображень та голосу також зумовлюють необхідність прискорення реалізації дискретне перетворення Фур'є над зображеннями чи акустичними сигналами.

В багатьох випадках перетворення Фур’є має реалізовуватися на простих портативних мікроконтролерах, які відіграють роль термінальних пристроїв і мають вбудовані засоби роботи з глобальними мережами. Для таких пристроїв, як правило, суттєвим є час виконання перетворення Фур’є і, відповідно, вони можуть для досягнення потрібних часових показників використовувати віддалені обчислювальні потужності, які здатні реалізувати дискретне перетворення Фур’є в реальному часі.

Наведені чинники зумовлюють актуальність розробок способів такого шифрування сигналів перед їх передачею в віддалені комп’ютерні системи для швидкого виконання перетворення Фур’є, яке унеможливлює доступ до сигналів та зображень з боку сторонніх осіб.

Таким чином, тема бакалаврської роботи, направленої на створення методу захищеної реалізації дискретного перетворення Фур’є на віддалених комп’ютерних системах є актуальною для сучасного етапу розвитку комп’ютерних технологій.

РОЗДІЛ 1
АНАЛІЗ ОБЧИСЛЮВАЛЬНИХ ПРОЦЕДУР ПЕРЕТВОРЕННЯ ФУР'Є ТА ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЇХ ЗАХИЩЕНОЇ РЕАЛІЗАЦІЇ

На сучасному етапі розвитку ІТ-індустрії, задачі цифрової обробки сигналів являються одними з найбільш масових задач сучасних комп'ютерних технологій. Левова частка прикладних задач, пов'язаних з цифровою обробкою сигналів виконується в режимі реального часу. Таким чином, процес виконання обчислень цифрової обробки сигналів підлягають жорстким вимогам. Для підвищення швидкості рівня реалізації базових операцій цифрової обробки сигналів, в тому числі, дискретного перетворення Фур'є, були створені запущені мікросхеми, які за рахунок розпаралелювання обчислень на апаратному рівні вирішують задачі з прискорення обробки [5]. В процесі програмної реалізації базових операцій цифрової обробки сигналів, широко використовуються можливості спеціалізованих графічних процесорів [6]. З появою такого унікального технічного феномену як прогресивні хмарні технології, процес обробки даних надає широкому колу користувачів практично необмежені обчислювальні потужності для вирішення різноманітних прикладних задач, в тому числі задач цифрової обробки сигналі і, зокрема, прямого та зворотного дискретного перетворення Фур'є. Однак факт широкого використання цієї можливості, яку надають сучасні технології, стримується незахищеністю даних при їх передачі та обробці на непідконтрольних і потенційно доступних зловмисникам віддалених комп'ютерних системах. Дане явище стимулює сучасних спеціалістів проводити багаторазові дослідження напрямків захищеності реалізації віддаленої цифрової обробки сигналів.

1.1 Огляд обчислювальних процедур перетворення Фур'є

Як зазначалося вище, основотворчою умовою здійснення операцій цифрової обробки сигналів є дискретне перетворення Фур'є. Воно також лежить в основі технологій обробки такого формату сигналів як зображення та аудіо. Дискретне перетворення Фур'є реалізує перетворення послідовності цифрових вимірів сигналу через певні проміжки часу в спектральне представлення сигналу, у вигляді набору амплітуд та фаз синусоїд, сума яких відтворює сигнал згідно з фундаментальною теоремою Фур'є.

З розвитком хмарних технологій, процес обчислення дискретного перетворення Фур'є виконується з меншим проміжком часу, що надає сучасному користувачеві доступ до глобальних мереж з практично необмеженими обчислювальними ресурсами. Ці можливості активно залучаються для вирішення широкого кола прикладних задач користувача. Парадокс в тому, що саме головні переваги хмарних технологій: обчислювальна потужність та загальнодоступність є в той самий час причиною недоліків і проблем. Особливо це стосується таких аспектів як втручання зловмисників, захищеності оброблюваної інформації та стійкості віддаленої обчислювальної системи.

Проведений теоретичний аналіз методичної та наукової літератури показав, що для більшості практичних застосувань дискретних перетворень Фур'є дані, які оброблюються, носять конфіденційний характер.

Таким чином, наукова задача організації захищеної реалізації ДПФ на віддалених обчислювальних потужностях є важливою та актуальною для сучасного етапу розвитку інформаційних технологій

Базовими операціями аналізу та обробки зображень є дискретне перетворення Фур'є (ДПФ) та швидке перетворення Фур'є (ШПФ). Тому для цих класів процедур обробки зображень потрібно розробити методи захищених реалізацій на віддалених процесорних засобах хмарних систем.

Проведений аналіз показав, що метод інтервального шифрування, запропонований в роботі для задач захищеної організації та фільтрації на віддалених комп'ютерних потужностях, не може бути ефективно застосований для виконання операцій перетворення Фур'є. Специфіка цих операцій вимагає розробки спеціальних методів їх захищеної реалізації.

Сучасні дослідження в області перетворення Фур'є направлені на активну реалізацію захищеного дискретного перетворення, але пояснити це можна наступним чином. Теоретично, будь-який сигнал, заданий сукупністю вимірів через рівний інтервал часу можна представити у вигляді суми синусоїд, частоти яких утворюють послідовність ω, 2·ω, 3·ω, 4·ω …. які мають певні амплітуди A_1, A_2,…, і розташовані в певних фазах φ_1, φ_2, φ_3, …. Розглянемо полярність даного питання. Цілком зрозуміло, що, чим більше синусоїд використано для представлення аналогового сигналу, тим вища якість представлення цього сигналу. З іншого боку, чим більше синусоїд використовується для представлення аналогового сигналу, тим більший об'єм обчислень потребує реалізація дискретного перетворення Фур'є.

Відповідно, вхідними даними для ДПФ є масив $x_0, x_2, \ldots x_{n-1}$ виміряних значень сигналу через фіксовані проміжки часу. В результаті перетворення отримується вихідний масив n комплексних чисел $y_0, y_2, .., y_{n-1}$, компоненти яких являють амплітуду та фазу синусоїд, сума яких відтворює заданий вхідний сигнал. Ці обчислення виконуються відповідно до наступної формули [6]:

$$\forall k \in \{0,1,\ldots n\text{-}1\}: \; y_k = \sum_{l=0}^{n-1} x_l \cdot W_n^{lk}, \quad \text{де } W_n = e^{-j\cdot\frac{2\pi}{n}}. \qquad (1.1)$$

Наведена формула (1.2) дозволяє отримати компоненти синусоїдальних сигналів з частотами ω, 2·ω, 3·ω …. в комплексному вигляді. Для багатьох практично важливих застосувань більш зручним є отримання кожної з цих компонент у вигляді двох окремих складових: реальної та уявної. При цьому

реальні складові $r_0,r_1,\ldots,r_{n-1}$ компонент синусоїдальних сигналів з частотами ω, 2·ω, 3·ω …. обчислюються за формулою:

$$\forall i \in \{0,1,...,n-1\} : r_i = \frac{1}{n}\sum_{l=0}^{n-1} x_l \cdot \cos\frac{2\cdot\pi\cdot l\cdot i}{n}. \qquad (1.2)$$

Уявні складові $m_0,m_1,\ldots,m_{n-1}$ компонент синусоїдальних сигналів з частотами ω, 2·ω, 3·ω …. обчислюються за формулою:

$$\forall i \in \{0,1,...,n-1\} : m_i = \frac{1}{n}\sum_{l=0}^{n-1} x_l \cdot \sin\frac{2\cdot\pi\cdot l\cdot i}{n} \quad . \qquad (1.3)$$

В результаті перетворення отримується вихідний масив *n* комплексних чисел $y_0,y_2,..,y_{n-1}$, компоненти яких являють амплітуду та фазу синусоїд, сума яких відтворює заданий вхідний сигнал. Якщо позначити через r_i реальну компоненту y_i, а через m_i – уявну компоненту, через A_i – амплітуду *i*-того спектру, φ_i – зсув фази y_i , i=0,1,…,n-1, то відповідні величини обчислюються наступним чином. Амплітуди А синусоїдальних сигналів з частотами кратними ω обчислюються згідно з формулою:

$$\forall i \in \{0,1,...,n-1) : A_i = \sqrt{r_i^2 + m_i^2} \quad . \qquad (1.4)$$

Фазові зсуви φ синусоїдальних сигналів з частотами кратними ω обчислюються згідно з формулою

$$\forall i \in \{0,1,...,n-1\} : \varphi_i = arctg\frac{m_i}{r_i} \quad . \qquad (1.5)$$

Згідно з проведеними дослідженнями [7] найбільш ресурсоємка частина обчислень визначається формулами (1.2) та (1.3). Показано, що кількість операцій множення з плаваючою точкою і додавань з плаваючою точкою для реалізації цих формул дорівнює n^2.

1.2 Огляд відомих технологій захищених обчислень

Одним з основних недоліків хмарних технологій, що істотно обмежує їх застосування, є можливість несанкціонованого доступу до даних користувача

при їх передачі та обробці на віддалених обчислювальних потужностях. Над вирішенням даного питання було проведено значну кількість робіт. Основна проблема полягає в тому, що не існує єдиного підходу до захисту даних в процесі їх обробки. Фактично, переважна частина виконаних досліджень вирішує проблему захисту даних тільки для окремих класів обчислювальних задач, наприклад, для лінійної алгебри, обробки зображень і т.п. [2]. Широким фронтом ведуться дослідження, спрямовані на створення ефективної захищеної організації виконання в відкритих віддалених системах операції модулярного експоненціювання - базової процедури широкого класу протоколів захисту інформації [3]. Проведений аналіз показав наступний результат - рішення задачі захищеного модулярного експоненціювання полягає в поділі обчислень на дві частини. Одна з них, велика частина, виконується переважно на віддалених обчислювальних потужностях, інша, менша за обсягом - на комп'ютерній системі користувача. В якості критеріїв ефективності організації віддаленого обчислення модулярной експоненти логічним видається використовувати:

- рівень захищеності, мірою якого є обсяг ресурсів, які потрібно витратити для відновлення секретних компонент операції за кодами переданих у відкриту систему даних;
- співвідношення кількості операцій що виконуються на процесорі користувача при використанні віддалених обчислень і кількості операцій за умови, що все модулярне експоненціювання здійснюється користувачем.

Останній критерій дозволяє оцінити можливість прискорення реалізації мережевих протоколів захисту інформації за рахунок використання можливостей сучасних хмарних технологій без шкоди для інформаційної безпеки.

В роботі [4] запропоновано метод віддаленого обчислення модулярного експоненціювання на основі випадкового поділу коду експоненти E на групи розрядів. Це дозволяє організувати обчислення $A^E \bmod M$ у вигляді добутків часткових експонент, які можу обчислюватися незалежно від рівня

потужності віддалених обчислюваних хмар. Користувач самостійно здійснює формування добутку $A^E \text{mod} M$. Для захисту компоненти А-даних, використовується виконання кількох перших кроків експоненціювання на комп'ютері користувача.

Істотною перевагою розглянутого методу є те, що в повній мірі можуть використані можливості багатопроцесорних віддалених систем із паралельного обчислювання часткових експонент. В роботі [4] на основі теоретичних і експериментальних даних встановлено, що описаний метод дозволяє приблизно в три рази реально підвищити продуктивність виконання модулярного експоненціювання.

Запропонований в даній роботі метод віддаленого обчислення модулярной експоненти полягає у поетапному розкладанні компонента А[3]. Такий підхід дозволяє розкласти загальне значення обчислення $A^E \text{mod} M$ на ряд експонент, які оперують з модифікованими даними і можуть також обчислюватися паралельно на віддалених обчислювальних потужностях, що дозволяє прискорити процес модулярного експоненціювання приблизно в 2-3 рази. Ще один цікавий підхід запропонований в роботі [2]. Акумулюючи дані дослідження може виокремити певний факт - основний акцент в цих дослідженнях зроблений на тому, щоб користувач міг не тільки віддалено виконати модулярне експоненціювання в закритому режимі, а й опосередковано контролювати правильність виконаних операцій.

Незакінченим питанням залишилось формування коректного результату в спеціальних методах шиврування на вирішення якого направлені виконані до теперішнього часу дослідження, аби віднайти спосіб дешифрування результатів віддаленої обробки зашифрованих даних. На сьогоднішній день розвитку ІТ не існує універсальних методів шифрування даних перед їх віддаленою обробкою, які не залежать від операцій обробки сигналів. Це означає, що для кожного виду обробки сигналів слід окремо розробляти метод шифрування та дешифрування.

В роботі [8] запропоновано методи захищеної реалізації масових операцій обробки зображень - медіанної та середньоарифметичної фільтрації. В основі цих методів покладено інтервальне шифрування точок зображення перед передачею його для обробки в хмарних системах. Метод забезпечує виконання медіанної фільтрації на віддалених відкритих комп'ютерних системах, закриваючи при цьому доступ до справжнього зображення.

Проведений аналіз показав, що метод інтервального шифрування запропонований в роботі для задач захищеної організації фільтрації на віддалених комп'ютерних потужностях не може бути ефективно застосований для виконання операцій перетворення Фур'є. Специфіка цих операцій вимагає розробки спеціальних методів їх захищеної реалізації.

1.3 Огляд відомих технологій захищеної реалізації перетворення Фур'є та аналіз можливостей її вдосконалення

Важливість впровадження захищеної дискретної трансформації Фур'є та актуальність питань, що вирішуються перетворенням Фур'є, призвели до інтенсивного дослідження цієї теми.

Зокрема, в роботі [9] пропонується метод шифрування даних, над якими віддалено виконується дискретне перетворення Фур'є. При цьому, алгоритми, засновані на модульній експозиції, використовуються для шифрування даних. Це дозволяє гнучко регулювати рівень безпеки віддаленої реалізації дискретного перетворення Фур'є.Крім того, в розробці запропоновані ефективні механізми контролю функціональної коректності виконання віддаленого дискретного перетворення Фур'є на непідконтрольних обчислювальних платформах. Разом з тим, використання в якості механізму шифрування модулярного експоненціювання помітно ускладнює вибір ключів та має наслідком значну обчислювальну складність реалізації дискретного перетворення Фур'є, яка в декілька разів перевищує складність реалізації

дискретного перетворення Фур’є за формулами (1.2) і (1.3). Суттєву проблему становить генерація ключів в запропонованому методі, яка потребує також значних обчислювальних ресурсів. Якщо припустити, що ключі використовуються неодноразово, це призводить до зниження рівня безпеки, враховуючи, що це відкриває зловмиснику набагато більше можливостей зламати шифр-код. Використання ж одноразових ключів в запропонованій розробці призводить до збільшення витрати обчислювальних ресурсів для реалізації дискретного перетворення Фур’є.

Таким чином, головним недоліком відомого способу реалізації захищеного дискретного перетворення Фур'є на віддалених обчислювальних платформах є значна обчислювальна складність реалізації дискретного перетворення Фур'є в хмарі, що не дозволяє реалізувати ці обчислення в режимі реального часу. Проблема полягає у складності генерації ключів, яка виконується безпосередньо користувачем..

Іншим відомим методом захищеної реалізації дискретного перетворення Фур'є на віддалених комп’ютерних системах є використання адитивного маскування.

Для здійснення безпечного обчислення дискретного перетворення Фур'є, цей метод включає виконання наступної послідовності дій:

1) Генерації випадкових комплексних чисел $q_0, q_2, \ldots q_{n-1}$, що являють собою послідовність масок для відліків сигналу X.

2) Адитивне маскування відліків сигналу X шляхом додавання послідовності масок до вхідної послідовності. В результаті користувач отримує послідовність замаскованих відліків сигналу $x'_0, x'_2, \ldots x'_{n-1}$:

$$\forall\, l \in \{0,1,\ldots,\ n-1\}:\ x'_l = x_l + q_l .$$

3) Отриману послідовність замаскованих відліків $x'_0, x'_2, \ldots x'_{n-1}$ користувач відправляє на віддалену комп’ютерну систему по відкритим каналам передачі даних.

Віддалена комп'ютерна система виконує над отриманою послідовністю $x'_0, x'_1, \ldots x'_{n-1}$ дискретне перетворення Фурє у відповідності з формулами:

$$\forall k \in \{0,1,\ldots n\text{-}1\}: y_k' = \sum_{l=0}^{n-1} x_l' \cdot W_n^{k \cdot l}, \tag{1.5}$$

Отриману в результаті послідовність $y'_0, y'_1, \ldots, y'_{n-1}$ система відсилає користувачеві.

4) З отриманням послідовності $y'_0, y'_1, \ldots y'_{n-1}$ від системи користувач виконує формування інверсної послідовності $x''_0, x''_1, \ldots x''_{n-1}$ шляхом віднімання послідовності масок від вхідної послідовності: $\forall i \in \{0,1,\ldots,n\text{-}1\}: x_i'' = x_i - q_i$.

5) Отриману послідовність $x'''_0, x''_2, \ldots x''_{n-1}$ користувач відправляє на віддалену комп'ютерну систему по відкритим каналам передачі даних.

6) Віддалена комп'ютерна система виконує над отриманою послідовністю $x'_0, x'_1, \ldots x'_{n-1}$ дискретне перетворення Фур'є у відповідності з формулами:

$$\forall k \in \{0,1,\ldots n\text{-}1\}: y_k'' = \sum_{j=0}^{n-1} x_j'' \cdot W_n^{k \cdot j}, \tag{1.6}$$

Отриману в результаті послідовність $y''_0, y''_1, \ldots, y''_{n-1}$ чисел з плаваючою точкою система надсилає користувачеві.

6) Користувач формує вихідну послідовність дискретне перетворення Фур'є на власній обчислювальній платформі шляхом поелементного обчислення середнього арифметичного отриманих з хмари двох послідовностей $y'_0, y'_1, \ldots, y'_{n-1}$ та $y''_0, y''_1, \ldots, y''_{n-1}$ згідно з наступною формулою:

$$\forall i \in \{0,1,\ldots,n-1\}: y_i = \frac{y_i' + y_i''}{2}. \tag{1.7}$$

Конструктивність описаної організації безпечного обчислення дискетного перетворення Фур'є на віддаленій обчислювальній потужності можна довести наступним чином.

Перша результуюча послідовність $y'_0, y'_1, \ldots, y'_{n-1}$ може бути представлена у вигляді:

$$\forall j \in \{0,1,...,n-1\} : y'_j = \sum_{l=0}^{n-1} (x_l + m_l) \cdot W_n^{k-l} = \sum_{l=0}^{n-1} x_l \cdot W_n^{k-l} + \sum_{l=0}^{n-1} m_l \cdot W_n^{lk} \quad . \qquad (1.8)$$

Друга послідовність $y''_0, y''_1,\ldots,y''_{n-1}$ отриманих користувачем результатів може бути представлена в такому виді [8]:

$$\forall j \in \{0,1,...,n-1\} : y''_j = \sum_{l=0}^{n-1} (x_l + m_l) \cdot W_n^{k-l} = \sum_{l=0}^{n-1} x_l \cdot W_n^{k-l} + \sum_{l=0}^{n-1} m_l \cdot W_n^{lk} \quad . \qquad (1.9)$$

Таким чином, користувач, обчислюючи середнє арифметичне двох отриманих від віддаленої комп'ютерної системи послідовностей $y'_0, y'_1,\ldots,y'_{n-1}$ та $y''_0, y''_1,\ldots,y''_{n-1}$ за формулою (1.7) формує наступну послідовність результуючих відліків сигналу, для кожного з яких виконується наступне [8]:

$$\forall k = 0,1,...,n-1 : y_k = \frac{y'_k + y''_k}{2} = \frac{\sum_{l=0}^{n-1} x_l \cdot W_n^{k-l} + \sum_{l=0}^{n-1} m_l \cdot W_n^{k-l}}{2} + \qquad (1.10)$$

$$+ \frac{\sum_{l=0}^{n-1} x_l \cdot W_n^{k-l} - \sum_{l=0}^{n-1} m_l \cdot W_n^{k-l}}{2} = \sum_{l=0}^{n-1} x_l \cdot W_n^{k-l}$$

Аналіз виразу (1.10) показує, що отриманий результат співпадає з результатами дискретного перетворення Фур'є виконаного над оригінальними відліками сигналу X по формулі (1.1).

Ефективність описаного відомого методу захищеної реалізації дискретного перетворення Фур'є на віддалених обчислювальних потужностях оцінюється:

- зменшенням обчислювальної складності операцій, що виконуються безпосередньо користувачем на власній обчислювальній платформі.

- рівнем захищеності вихідних даних, які передаються користувачем на віддалену і потенційно незахищену комп'ютерну систему.

При виконанні дискретного перетворення Фур'є на обчислювальній платформі користувача, кількість операцій множення і додавання $2 \cdot n^2$. Враховуючи, що згідно з [11] тривалість операцій процесорного множення в

30 раз більша за тривалість операції додавання, то загальний час виконання дискретного перетворення Фур'є визначається як:

$$T_k = \left(2 \cdot (30 \cdot n)^2 + 2n^2\right) \cdot \tau_д \approx 1800 \cdot n^2 \cdot \tau_д, \ , \qquad (1.11)$$

де $\tau_д$ час виконання операції додавання чисел з плаваючою точкою.

При реалізації описаного методу користувач виконує операції додавання випадкової послідовності (*n* операцій додавання), віднімання випадкової послідовності (*n* операцій типу додавання), а також обчислення середнього арифметичного (*n* операцій додавання і *n* операцій ділення на два). Оскільки операція зсуву виконується значно швидше операції додавання, то можна вважати, що час виконання користувачем дискретного перетворення Фур'є обчислюється за наступною формулою [9]:

$$T_0^{'} = 3 \cdot n \cdot \tau_д . \qquad (1.12)$$

Відповідно, описаний методу захищеної реалізації дискретного перетворення Фур'є дозволяє прискорити обчислення в ν раз, а числове значення ν визначається наступною формулою [9]:

$$\nu = \frac{T_k}{T_0^{'}} = 900 \cdot n \ . \qquad (1.13)$$

Таким чином, згідно (1.13), описаний метод забезпечує прискорення виконання дискретного перетворення Фур'є користувачем приблизно на 4 порядки. Проведені експериментальні дослідження показали, що реальне збільшення швидкодії при реалізації перетворення Фур'є становить близько $6 \cdot 10^3$. Це свідчить про високу ефективність застосування описаного методу захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах на основі хмарних технологій.

Несанкціонований доступ до даних користувача за допомогою описаного методу може бути реалізований як на етапі їх передачі по мережі, так і безпосередньо на віддалених комп'ютерних системах, які виконують обчислення, пов'язані з перетворенням Фур'є.

Рівень захисту даних оцінюється кількістю обчислювальних ресурсів, необхідних зловмиснику для незаконного доступу до даних.

При застосуванні описаного методу для одиночної операції дискретного перетворення Фур'є вимога забезпечення захищеності операндів та результатів не забезпечується, оскільки зловмисних, перехопивши послідовності x_0', x_1',…,x_{n-1}' та x_0'', x_1'',…,x_{n-1}'' достатньо просто відновить значення вхідної послідовності x_0, x_1,…,x_{n-1} для перетворення Фур'є шляхом поелементного обчислення середнього арифметичного двох перехоплених послідовностей.

Проте аналіз практичних застосувань операції дискретного перетворення Фур'є для обробки зображень [11] показує, що реально виконується потік вказаних операцій. Тобто практично завжди виконується послідовність з a операцій дискретного перетворення Фур'є. При виконанні вказаного потоку описаний метод передбачає:

- використання для кожної з h реалізацій дискретного перетворення Фур'є окремих послідовностей масок ;

- генерацію користувачем секретних, не співпадаючих між собою послідовності $v_1,v_2,\ldots,v_h$ та $w_1,w_2,\ldots,w_h$, $\forall l \in \{1,2,\ldots,a\}$: $v_l \in \{1,2,\ldots,a\}$, $w_l \in \{1,2,\ldots,\phi\}$ відправки на віддалені обчислювальні потужності вхідних даних для кожної з a реалізацій дискретного перетворення Фур'є. Ці послідовності є секретними і визначають порядок отримання результатів користувачем.

- обчислення згідно формули (1.7) результату l-ї реалізації дискретного перетворення Фур'є здійснюється користувачем після отримання відповідних результатів від віддалених обчислювальних потужностей.

Відповідно, зловмиснику, для того, щоб відновити вхідні дані потоку операцій дискретного перетворення Фур'є потрібно виявити порядок вхідних послідовностей з потоку $2 \cdot a$ посилок даних користувача. Очевидно, що для цього потрібно здійснити перебір об'ємом $2 \cdot a^2$ варіантів, для кожної з яких

необхідно виконати дві операції дискретного перетворення Фур’є, що потребує $2 \cdot n^2$ операцій множення з плаваючою точкою.

Таким чином, для отримання незаконного доступу до даних одного перетворення Фур’є, що виконується на віддалених комп’ютерних потужностях, потрібний зловмиснику об’єм ресурсів оцінюється часом виконання $8 \cdot a^2 \cdot n^2$ операцій множення. Враховуючи, що в реальних системах [12], значення n=64, а a=10^3, , то об’єм ресурсів для отримання незаконного доступу оцінюється часом виконання 10^9 операцій множення, що для більшості застосувань робить злам запропонованого механізму захисту практично недоцільним.

Описаний метод [8] по суті реалізує потокове шифрування даних, що надсилаються користувачем у віддалені комп'ютерні системи, де перетворення Фур'є здійснюються безпосередньо, а також дешифрування отриманих результатів. Головною перевагою цього методу [8] є простота операцій шифрування та дешифрування даних, що забезпечує низький рівень витрат обчислювального часу на виконання операцій, пов’язаних з захистом інформації.

Основним недоліком відомого способу [8] захищеної реалізації перетворення Фур'є є те, що він підходить лише для обмеженого класу задач, де існує дійсно великий потік проблем дискретного перетворення Фур'є. Це звужує сферу його ефективного застосування.

Таким чином, відомі методи захищеної реалізації перетворення Фур’є на віддалених комп’ютерних системах на забезпечують належної ефективності захисту. Це вимагає створення нових методів вирішення цієї технічної задачі.

Метою розробки є створення методу безпечної реалізації дискретного перетворення Фур'є на віддалених комп'ютерних системах з використанням хмарних технологій, який не потребує значних обчислювальних ресурсів і дозволяє реалізовувати віддалені обчислення в режимі реального часу.

Висновки до розділу 1

В результаті виконання досліджень, направлених на аналіз обчислювальних процедур дискретного перетворення Фур'є в плані можливостей його захищеної реалізації на віддалених і потенційно небезпечних комп'ютерних системах можна зробити такі висновки:

1. Визначено, що значна частина операцій цифрової обробки сигналів в сучасних засобах комп'ютерної обробки інформації базується на прямому та зворотному дискретному перетворенні Фур'є. Аналіз динаміки розвитку таких систем показав, що має місце тенденція до підвищення якості обробки за рахунок збільшення числа відліків сигналів, а також більш жорскими стають вимоги до оперативності виконання операцій дискретного перетворення Фур'є. Показано, що їх реалізація може бути значною мірою прискорена за рахунок розпаралелювання обчислювального процесу з залученням віддалених обчислювальних потужностей в рамках сучасних хмарних технологій. Основною завадою на щляху реалізації цих можливостей є незахищеність даних користувачів при їх передачі по потенційно відкритим каналам Інтернет та обробки на непідконтрольних віддалених обчислювальних потужностях.

3. Визначені критерії ефективності захищеної реалізації операцій дискретного перетворення Фур'є на віддалених обчислювальних потужностях. В якості таких критеріїв пропонується використовувати рівень захищеності даних про сигнал під час їх передачі та обробці на непідконтрольних користувачам обчислювальних потужностях, а також рівень зменшення об'єму обчислень, що виконуються на обчислювальній платформі користувача.

4. Критичний огляд з позицій визначених критеріїв, існуючих методів захищеної реалізації дискретного перетворення Фур'є на віддалених обчислювальних системах показав, що вони не в повній мері задовольняють

вимогам сьогодення. Зокрема показано, що існуючі підходи до гомоморфного шифрування сигналів під час їх віддаленої обробки з використанням дискретного перетворення Фур'є не задовольняють вимогам надійного унеможливування незаконного доступу до даних.

5. Показано, що існують потенційні можливості для подальшого підвищення ефективності захищеної реалізації обробки дискретного перетворення Фур'є на віддалених комп'ютерних системах за рахунок вдосконалення методів гомоморфного шифрування сигналів.

РОЗДІЛ 2
РОЗРОБКА МЕТОДУ ЗАХИЩЕНОЇ РЕАЛІЗАЦІЇ ПЕРЕТВОРЕННЯ ФУР'Є НА ВІДДАЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

Однією з найбільш поширених прикладних обробки сигналів є швидке перетворення Фур'є. Таке перетворення дозволяє приводити сигнали різної природи (зображення, голосі сигнали. сейсмограми, радіосигнали) стандартного представлення у вигляді наборів дійсних чисел, що дає змогу порівнювати та аналізувати сигнали, здійснювати їх розпізнавання.

Висока ресурсоємність процедур швидкого перетворення Фур'є, визначається великою кількістю точок вимірів сигналу диктує практичну доцільність використання потужних багатопроцесорних віддалених комп'ютерних систем. Аналіз обчислювальних процедур швидкого перетворення Фур'є [12] показує, що вона допускає широке розпаралелювання, що також педалює доцільність залучення віддалених багатопроцесорних потужних систем. Ще одним чинником на користь такої організації обробки сигналів з використання перетворень Фур'є є те, що дуже часто існують жорсткі часові обмеження на його реалізацію в практичних застосуваннях.

Серйозною перепоною на шляху широкого використання можливостей хмарних обчислень для реалізації перетворень Фур'є виступає характер обмежень доступу до сигналів та зображень. Саме це суттєвим чином обмежує їх обробку у відкритих системах, в тому числі GRID-системах. Відповідно, виникає практична потреба в організації захищеної реалізації перетворень Фур'є в сучасних відкритих розподілених комп'ютерних системах великої потужності [13] в рамках хмарних технологій. Основна вимога при організації захищеної реалізації перетворень Фур'є на віддалених і практично непідконтрольних обчислювальних потужностях полягає в тому, що воно має

практично унеможливити доступ до оригінальних сигналів в процесі їх передачі і при обробці.

Для розробки ефективного методу захищеного віддаленого обчислень, пов’язаних з перетворенням Фур’є на віддалених комп'ютерних потужностях потрібно визначити теоретичні можності для вирішення поставленої задачі. На основі виявлених можливостей виконати аналіз шляхів їх реалізації і, відповідно, вибрати найкращий, за встановленими критеріями, варіант, який розробити у вигляді формалізованого методу. Потрібно теоретично та експериментально дослідити ефективність розробленого методу, як в плані визначення досягнутого рівня захищеності, так і в плані підвищення швидкодії за рахунок використання віддалених обчислювальних потужностей.

2.1 Теоретичний аналіз можливостей захищеного перетворення Фур’є

Дискретне перетворення Фур’є здійснює перехід зображення від конфігураційного простору до частотного простору. Для багатьох практично важливих застосувань це перетворення має здійснювати в режимі реального часу. Тому, існують жорсткі вимоги до часу виконання дискретного перетворення Фур’є. Важливість швидкого переходу представлення сигналу від конфігураційного простору до частотного простору зумовила появу широкої номенклатури спеціалізованих мікросхем дискретного перетворення Фур’є для прискореної апаратної цієї важливої для практики операції.

Будь-який сигнал, заданий сукупністю вимірів через рівний інтервал часу можна представити у вигляді суми синусоїд, частоти яких утворюють послідовність ω, $2\cdot\omega$, $3\cdot\omega$, $4\cdot\omega$ …. які мають певні амплітуди A_1, A_2,…, і зсунуті на певні фази φ_1, φ_2, φ_3, ….

Вхідними даними для ДПФ є масив $x_0, x_2, \ldots x_{n-1}$ виміряних значень сигналу через фіксовані проміжки часу. В результаті перетворення отримується вихідний масив n комплексних чисел $y_0, y_2, .., y_{n-1}$, компоненти яких являють

амплітуду та фазу синусоїд, сума яких відтворює заданий вхідний сигнал. Якщо позначити через r_i реальну компоненту y_i, а через m_i – уявну компоненту, через A_i – амплітуду i-того спектру, φ_i – зсув фази y_i , i=0,1,…,n-1, то відповідні величини обчислюються через наступні формули:

$$r_i = \frac{1}{n}\sum_{j=0}^{n-1} x_j \cdot \cos\frac{2\cdot\pi\cdot j\cdot i}{n} \qquad (2.1)$$

$$m_i = \frac{1}{n}\sum_{j=0}^{n-1} x_j \cdot \sin\frac{2\cdot\pi\cdot j\cdot i}{n}$$

По отриманими за формулами (2.1) значеннями реальних компонент і уявних компонент синусоїдального сигналу з частотою $i\cdot\omega$, можна обчислити амплітуду цього сигналу, а також його фазовий зсув за формулами:

$$A_i = \sqrt{r_i^2 + m_i^2} \qquad (2.2)$$

$$\varphi_i = arctg\frac{m_i}{r_i}$$

Згідно з проведеними дослідженнями [13] найбільш ресурсоємка частина обчислень визначається формулами (2.1). Цілком очевидно, що кількість операцій множення з плаваючою точкою і додавань з плаваючою точкою для реалізації формул (2.1) дорівнює n^2. Це означає, що зі збільшенням кількості n число операцій множення та додавання з плаваючою точкою швидко зростає. Відповідно, потрібно організувати віддалене обчислення формул (2.1) на багатопроцесорних обчислювальних системах з метою зменшення часу виконання дискретного перетворення Фур'є. З структури формул (2.1) цілком очевидно, що вони можуть обчислюватися паралельно на n процесорах.

Зрозуміло, що косинуси та синуси не залежать від значень $x_0, x_2, \ldots x_{n-1}$ і їх можна вважати постійними числами, значення яких визначаються лише індексами. Тому, попередньо можуть бути обчислені складові формул (2.1) у вигляді набору коефіцієнтів, які, в подальших дослідженнях можуть

вважатися постійними. Обчислення коефіцієнтів може бути здійснене згідно наступних формул:

$$\forall i, j \in \{0,2,...,n-1\} : a_{ij} = \frac{1}{n} \cdot \cos\frac{2 \cdot \pi \cdot j \cdot i}{n}. \qquad (2.3)$$

$$\forall i, j \in \{0,2,...,n-1\} : c_{ij} = \frac{1}{n} \cdot \sin\frac{2 \cdot \pi \cdot j \cdot i}{n}$$

Наприклад, для n=8 значення тригонометричних коефіцієнтів a для дискретного перетворення Фур'є, обчислені за формулами (2.3) наведені в таблиці 2.1.

Таблиця 2.1

Значення тригонометричних коефіцієнтів a дискретного перетворення Фур'є для n=8

j	i							
	0	1	2	3	4	5	6	7
0	1	1	1	1	1	1	1	1
1	1	0.7074	0.00079	-0.7063	-0.9999	- 0.7085	-0.00239	0.7051
2	1	0.0008	-1	-0.00239	1	0.004	1	-0.0056
3	1	-0.7063	-0.0024	0.7096	-1	0.7029	0.007	-0.713
4	1	-1	1	-1	1	-1	1	-1
5	1	-0.7085	0.004	0.7028	-1	0.7141	-0.0119	-0.6971
6	1	-0.0024	-1	0.0072	1	-0.012	-1	0.0167
7	1	0.7051	-0.0056	-0.713	-1	-0.6971	0.0167	0.720

З аналізу даних наведених в таблиці 2.1 цілком очевидно, що тригонометричні коефіцієнти дискретного перетворення Фур'є є симетричними відносно діагоналі. Це, теоретично, дозволяє прискорити обчислення формул (2.1). На практиці цифрової обробки сигналів ця можливість реалізована в формі швидкого перетворення Фур'є, яке дозволяє зменшити кількість операцій множення та додавання за рахунок використання властивостей симетрії коефіцієнтів дискретного перетворення Фур'є. При застосуванні

швидкого перетворення Фур'є використовується $n^2/2$ операцій множення з плаваючою точкою та така ж кількість - $n^2/2$ операцій додавання з плаваючою точкою. Тобто реальна обчислювальна складність реалізації формул (2.1) з використанням швидкого перетворення Фур'є зменшується удвічі.

Проте використання швидкого перетворення Фур'є при реалізації на віддалених багатопроцесорних системах не є ефективним в силу того, що воно не дозволяє досягти максимального розпаралелювання процесу обчислень. При використанні великої кількості процесорів пряме обчислення дискретного перетворення Фур'є забезпечує більшу швидкодію.

Якщо використовувати постійні коефіцієнти, що обчислюються за формулами (2.3), то базові формули (2.1) можуть спрощені до наступного вигляду :

$$r_i = \sum_{j=0}^{n-1} x_j \cdot a_{ij} \quad . \qquad (2.4)$$

$$m_i = \sum_{j=0}^{n-1} x_j \cdot c_{ij}$$

Потрібно організувати захищене перетворення Фур'є: тобто зашифрувати значення $x_0, x_2, \ldots x_{n-1}$, що передаються в хмару. Вважати, що в хмарі обчислюються значення $v_0, v_2, \ldots v_{n-1}$ та $w_0, w_2, \ldots w_{n-1}$ за формулами (2.4) та повертаються користувачеві, який має відновити справжні значення $r_0, r_2, \ldots r_{n-1}$ та $m_0, m_2, \ldots m_{n-1}$.

Як зазначалося вище, реалізація дискретного перетворення Фур'є на віддалених комп'ютерних багатопроцесорних системах відкриває широкі можливості для розпаралелювання обчислювального процесу. Теоретично, при використанні необмеженого числа процесорів, операції множення можуть виконуватися одночасно на $2 \cdot n^2$ процесорах. Крім того, для формування $2 \cdot n$ сум згідно з формулами (2.4) потрібно на $2 \cdot n$ процесорах виконали $\log_2 n$ операцій додавання. Таким чином, теоретично мінімальний час T_M виконання

дискретного перетворення Фур’є на віддалених комп'ютерних багатопроцесорних системах визначається формулою:

$$T_M = t_M + t_a \cdot \log_2 n\,, \qquad (2.5)$$

де t_M – час виконання операції множення з плаваючою точкою, а t_a – час здійснення операції додавання з плаваючою точкою.

Якщо виконувати дискретного перетворення Фур’є на одному процесорі, то час виконання перетворень Фур'є зазвичай характеризується числом множень та додавань, які потрібно виконати в процесі виконання цього перетворення. Цілком очевидно, для число множень при здійсненні дискретного перетворення Фур'є дорівнює n^2, а число додавань становить $n\cdot(n-1)$ [14]. Тобто чисельне значення часу $T_Б$ виконання дискретного перетворення Фур’є на одному процесорі визначається за такою формулою:

$$T_Б = n^2 \cdot t_M + n \cdot (n-1) \cdot t_a\,, \qquad (2.6)$$

Враховуючи, що для сучасних процесорів час виконання операції множення з плаваючою точкою приблизно в 30 раз більша за час виконання операції додавання з плаваючою точкою [15], то формула (2.6) може бути спрощена до наступного вигляду:

$$T_Б = (31 \cdot n^2 - n) \cdot t_a\,. \qquad (2.7)$$

Таким чином, залучення для виконання дискретного перетворення Фур’є віддалених багатопроцесорних обчислювальних систем з використанням можливостей хмарних технологій дозволяє прискорити обчислення в γ раз, причому чисельне значення γ визначається наступною формулою:

$$\gamma = \frac{T_Б}{T_M} = \frac{31 \cdot n^2 - n}{30 + \log_2 n}\,. \qquad (2.8)$$

Наприклад, при n=8 обчислене за формулою (2.8) значення γ становить 60, а при n=128 значення γ дорівнює вже 13724.

На практиці цифрової обробки сигналів дискретне перетворення Фур'є часто реалізується в формі швидкого перетворення Фур'є, яке дозволяє зменшити кількість операцій множення та додавання за рахунок використання властивостей симетрії коефіцієнтів дискретне перетворення Фур'є. При застосуванні швидкого перетворення Фур'є використовується [14] $n^2/2$ операцій множення з плаваючою точкою та така ж кількість - $n^2/2$ операцій додавання з плаваючою точкою. Відповідно, при використанні швидкого перетворення Фур'є час $T_Б'$ виконання перетворення визначається наступною формулою:

$$T_Б' = \frac{31 \cdot n^2}{2} \cdot t_a \ . \qquad (2.9)$$

Відповідно, при застосуванні на обчислювальній платформі користувача швидкого перетворення Фур'є чисельне значення коефіцієнту прискорення γ' визначається наступною формулою:

$$\gamma' = \frac{T_Б'}{T_M} = \frac{31 \cdot n^2 - n}{2 \cdot (30 + \log_2 n)} . \qquad (2.10)$$

Співставлення формул (2.8) і (2.10) показує, що при застосуванні на обчислювальній платформі користувача швидкого перетворення Фур'є коефіцієнт прискорення зменшується практично вдвоє.

З цього можна зробити два важливих висновки:

- Використання віддалених багатопроцесорних обчислювальних систем для прискорення обчислювальної реалізації дискретного перетворення Фур'є дає значний ефект в плані прискорення виконання обчислень, що дуже важливо для практичних застосувань, що функціонують в режимі реального часу;

- ефективність використання в рамках хмарних технологій віддалених багатопроцесорних обчислювальних систем для прискорення обчислювальної реалізації дискретного перетворення Фур'є зростає зі збільшенням значення розмірності перетворення - n.

Для реалізації цих переваг, які надають сучасні хмарні технології потрібно розробити метод, який унеможливлює несанкціонований доступ до чисельних значень відліків значення сигналу в процесі виконання над ними дискретного перетворення Фур'є на віддалених і непідконтрольних користувачеві комп'ютерних системах.

2.2. Метод захищеної реалізації дискретного перетворення Фур'є на віддалених багатопроцесорних комп'ютерних системах

Для досягнення поставленої мети пропонується наступний метод організації захисту даних відліків сигналу від несанкціонованого доступу до них з боку сторонніх осіб безпосередньо під час виконання дискретного перетворення Фур'є.

Базова ідея методу полягає в тому, що кожен відлік сигналу x_j, $j \in \{1,2,\ldots,n\}$ можна представити у вигляді суми або різниці двох величин: опорної та зміщення:

$$\forall j \in \{1,2,...,n\} : x_j = B_q \pm \delta_j , \qquad (2.11)$$

де B_q – одне, а саме q-те, значення опорної величини, δ_j - зміщення відносно цієї опорної величини.

Значення B_q належить до множини Ω з χ елементів $\Omega=\{B_1,B_2,\ldots,B_\chi\}$. Цим опорним значенням співвідносяться значення результатів перетворення Фур'є: $\Theta=\{U_1,U_2,\ldots,U_\chi\}$ та $\Psi=\{W_1,W_2,\ldots,W_\chi\}$. Відповідно, чисельні значення елементів множин Θ та Ψ обчислюються у відповідності з наступними формулами:

$$\forall l \in \{1,2,...,w\} : U_l = \sum_{j=0}^{n-1} B_j \cdot a_{ij},$$
$$W_l = \sum_{j=0}^{n-1} B_j \cdot c_{ij} \qquad . \qquad (2.12)$$

Значення опорних сигналів, що складають множину Ω вибираються таким чином, щоб в найбільшій степені спотворити характер домінуючого типу

корисного сигналу X. Для кожної сфери практичного використання цифрової обробки сигналів можна виділити характерні властивості спектру сигналів. Відповідно опорні сигнали вибираються таким чином, щоб максимально спотворити спектр цих сигналів. Після вибору множини Ω здійснюються обчислення компонент множин Θ та Ψ з використанням формул (2.12) зі збереженням результатів в пам'яті. Слід зазначити, що ці обчислення здійснюються в некритичному з точки зору часу режимі з використанням обчислювальної платформи користувача.

В таблиці 2.2 в якості прикладу при n=8 наведені значення одного із опорних сигналів B та відповідні цьому сигналу компоненти множин Θ та Ψ, обчислені з використанням формул (2.12).

Таблиця 2.2

Значення результатів перетворення Фур'є для базового набору відліків

j	0	1	2	3	4	5	6	7
B_j	2.5	3.2	1.8	2.6	3.3	4.3	4.6	1.2
U_j	2.5	-0.0016	-0.0007	-0.0006	0	0.0018	0.0055	0.004
W_j	0	0.0006	0.0007	0.0016	0.0026	0.0043	0.0054	0.00163

При здійсненні дискретного перетворення Фур'є над сигналом X, заданим n значеннями його відліків: $x_1,x_2,\ldots,x_n$ виконується наступна послідовність дій:

1. Випадковим чином вибирається один із опорних сигналів з множини Ω. Без втрати узагальнення можна вважати, що номер вибраного опорного сигналу дорівнює q .

2. Обчислюються значення зміщень $\delta_0,\delta_1,\ldots,\delta_{n-1}$ відліків сигналу X відносно вибраного опорного сигналу B_q згідно з наступною формулою:

$$\forall i \in \{0,1,...,n-1\} : \delta_i = x_i - B_{qi} . \qquad (2.13)$$

3. Отримані значення $\delta_0,\delta_1,\ldots,\delta_{n-1}$ надсилаються в віддалену комп'ютерну систему.

4. Віддалена система здійснює дискретного перетворення Фур'є над сукупністю відліків $\delta_0,\delta_1,\ldots,\delta_{n-1}$ у відповідності з формулами:

$$\begin{aligned} &\forall i \in \{0,1,...,n-1\} : Z_i = \sum_{j=0}^{n-1} \delta_j \cdot a_{ij}, \\ &Y_i = \sum \delta_j \cdot c_{ij} \end{aligned} \quad . \qquad (2.14)$$

5. Віддалена система повертає користувачеві обчислені значення $Z_0,Z_1,\ldots,Z_{n-1}$ та $Y_0,Y_1,\ldots,Y_{n-1}$.

6. Користувач відновлює справжні значення компонентів спектрального представлення сигналу X: $r_0,r_2,\ldots r_{n-1}$ та $m_0,m_2,\ldots m_{n-1}$ за допомогою наступних перетворень:

$$\forall i \in \{0,1,...,n-1\} : r_i = U_{qi} + Z_i, m_i = W_{qi} + Y_i \ . \qquad (2.15)$$

В результаті запропонованої процедури віддаленого дискретного перетворення Фур'є на стороні користувача виконуються в ході реалізації п.2. тільки $2 \cdot n$ операцій віднімання, в рамках обчислень по формулі (2.13), а також при здійсненні п.6 $2 \cdot n$ операцій додавання згідно формули (2.15). Всі інші операції по дискретному перетворенню Фур'є виконуються на віддаленій комп'ютерній системі. Коректність отриманих в результаті запропонованої процедури результатів може бути доведена наступними математичними викладками:

$$\begin{aligned} r_i = \sum_{j=0}^{n-1} x_j \cdot \alpha_{ij} = \sum_{j=0}^{n-1} (B_{qj} + \delta_j) \cdot a_{ij} = \sum_{j=0}^{n-1} B_{qj} \cdot a_{ij} + \sum_{j=0}^{n-1} \delta_j \cdot a_{ij} = \\ = U_{qj} + \sum_{j=0}^{n-1} \delta_j \cdot a_{ij} \end{aligned} \quad . \qquad (2.16)$$

$$m_i = \sum_{j=0}^{n-1} x_j \cdot c_{ij} = \sum_{j=0}^{n-1} (B_{qj} + \delta_j) \cdot c_{ij} = \sum_{j=0}^{n-1} B_{qj} \cdot c_{ij} + \sum_{j=0}^{n-1} \delta_j \cdot c_{ij} =$$

$$= W_{qj} + \sum_{j=0}^{n-1} \delta_j \cdot c_{ij}$$

При застосуванні розробленої процедури на стороні віддаленої комп'ютерної системи є лише набір $\delta_0,\delta_1,\ldots,\delta_{n-1}$ відліків сигналу X відносно вибраного опорного сигналу B_q, який без знання відліків вказаного опорного сигналу не може бути відновлений. Оскільки відліки опорного сигналу B_q обчислюються і зберігаються на стороні користувача, то сигнал X практично не може бути відновлений на стороні системи, яка здійснює віддалену процедури дискретного перетворення Фур'є.

Робота запропонованого методу ілюструється наступним прикладом для n=8. Нехай, сигнал X задається на стороні користувача набором відліків: $x_0,x_1,\ldots,x_7$ що мають такі значення: x_0=3.4; x_1=3.5; x_2=3.6; x_3=4.1; x_4=3.8; x_5=3.1; x_6=2.5; x_7=2.0. При здійсненні процедури дискретного перетворення Фур'є на стороні користувача у відповідності з формулами (2.4) можна отримати значення реальних R та умовних M складових, які однозначно описують спектр заданого сигналу X. В рамках прикладу, що розглядаються результати відповідних обчислень наведені в таблиці 2.3.

Таблиця 2.3

Значення результатів перетворення Фур'є для заданного набору відліків

j	0	1	2	3	4	5	6	7
X_j	3.4	3.5	3.6	4.1	3.8	3.1	2.5	2
R_j	3.4	-0.0017	-0.0014	-0.001	0	0.0013	0.003	0.0067
M_j	0	0.0007	0.0014	0.0025	0.003	0.003	0.003	0.0027

При здійсненні процедури дискретного перетворення Фур'є у відповідності з запропонованою і викладеною вище методикою. В рамках п.1

цієї методики користувач випадковим чином вибирає один із опорних сигналів з множини Ω. Можна припустити, що, наприклад, користувач обрав опорний сигнал, представлений вище в таблиці 2.2. В цій же таблиці 2.2. наведені результати дискретного перетворення Фур'є над цим опорним сигналом у вигляді набору U реальних складових його спектру та набору W уявних складових. Відліки обраного опорного сигналу B, а також значення наборів U реальних і уявних W складових його спектру приведені в другому, шостому та шостому рядках таблиці 2.4 відповідно. В першому рядку цієї таблиці наведені значення набору відліків заданого вхідного сигналу X.

У відповідності з п.2 розробленої процедури, користувач обчислює значення зміщень $\delta_0,\delta_1,\ldots,\delta_{n-1}$ відліків сигналу X відносно вибраного опорного сигналу B_q. Значення цих значень наведені в третьому рядку таблиці 2.4. Ці значення у вигляді набору D надсилаються користувачем згідно п.3 в віддалену комп'ютерну систему.

Таблиця 2.4

Значення проміжних даних та результатів перетворення Фур'є для заданого набору відліків при використанні запропонованого методу

j	0	1	2	3	4	5	6	7
X_j	3.4	3.5	3.6	4.1	3.8	3.1	2.5	2
B_j	2.5	3.2	1.8	2.6	3.3	4.3	4.6	1.2
D_j	0.9	0.3	1.8	1.5	0.5	-1.2	-2.1	0.8
Z_j	0.9	-0.0001	-0.0007	-0.0004	0	-0.0005	-0.0025	0.0027
Y_j	0	0.0006	0.0007	0.0016	0.0026	0.0043	0.0054	0.00163
U_j	2.5	-0.0016	-0.0007	-0.0006	0	0.0018	0.0055	0.004
W_j	0	0.0006	0.0007	0.0016	0.0026	0.0043	0.0054	0.00163

R'_j	3.4	-0.0017	-0.0014	-0.001	0	0.0013	0.003	0.0067
M'_j	0	0.0007	0.0014	0.0025	0.003	0.003	0.003	0.0027

На віддаленій системі в рамках виконання п.4 здійснюється дискретне перетворення Фур'є над надісланою користувачем сукупністю відліків $\delta_0,\delta_1,\ldots,\delta_{n-1}$. В результаті перетворення Фур'є на віддалений комп'ютерній системі отримуються набори Z реальних і уявних Y складових спектру сигналу D. Числові дані набору Z реальних складових і набору Y уявних складових спектру D отриманих в результаті дискретне перетворення Фур'є наведені в четвертому та п'ятому рядках таблиці 2.4. Ці набори чисел повертаються віддаленою системою користувачеві.

Користувач, по отриманню числових даних набору Z реальних складових і набору Y уявних складових спектру D в рамках п. 6 запропонованої процедури відновлює справжні значення компонентів спектрального представлення сигналу X: а саме: набору R реальних складових і набору M уявних складових спектру сигналу X. Ці набори, обчислені за формулою (2.15) наведені в восьмому та дев'ятому рядках таблиці 2.4.

Порівняння даних цих двох стовпців таблиці 2.4 з двома останніми стовпцями таблиці 2.3, в якій містяться результати дискретного перетворення Фур'є за класичною процедурою, свідчить про те, що ці результати збігаються з результатами, отриманими в результаті виконання запропонованої процедури.

Оцінка ефективності має включати визначення двох критеріїв:

- рівень захищеності від спроб незаконного доступу до відліків сигналів, який визначається об'ємом ресурсів, потрібних для порушення захисту.

- коефіцієнтом ν прискорення обчислень, який визначається співвідношенням часу виконання перетворення Фур'є в базовому варіантів – $T_Б$, тобто згідно формул (2.1) та часу обчислень, пов'язаних з виконанням дискретного перетворення Фур'є за запропонованим методом, тобто часу, який

витрачається для здійснення цієї операції на обчислювальній платформі користувача – T_K:

$$\nu = \frac{T_Б}{T_K} \quad . \tag{2.17}$$

Час виконання перетворень Фур'є зазвичай характеризується числом множень та додавань, які потрібно виконати в процесі виконання цього перетворення. Цілком очевидно, для число множень при здійсненні дискретного перетворення Фур'є дорівнює n^2, а число додавань становить $n\cdot(n-1)$ [20].

$$T_Б = n^2 \cdot t_M + n \cdot (n-1) \cdot t_a \,, \tag{2.18}$$

де t_M – час виконання операції множення, а t_a – час здійснення операції додавання. Враховуючи, що для сучасних процесорів час виконання операції множення з плаваючою точкою приблизно в 30 раз більша за час виконання операції додавання з плаваючою точкою [21], то формула (2.9) може бути спрощена до наступного вигляду:

$$T_Б = (31 \cdot n^2 - n) \cdot t_a \,. \tag{2.19}$$

На практиці цифрової обробки сигналів дискретне перетворення Фур'є часто реалізується в формі швидкого перетворення Фур'є, яке дозволяє зменшити кількість операцій множення та додавання за рахунок використання властивостей симетрії коефіцієнтів дискретне перетворення Фур'є. При застосуванні швидкого перетворення Фур'є використовується [22] $n^2/2$ операцій множення з плаваючою точкою та така ж кількість - $n^2/2$ операцій додавання з плаваючою точкою. Відповідно, при використанні швидкого перетворення Фур'є час $T_Б'$ виконання перетворення визначається наступною формулою:

$$T_Б' = \frac{31 \cdot n^2}{2} \cdot t_a \quad . \tag{2.20}$$

При використання запропонованого методу, на обчислювальній платформі користувача виконується тільки $2 \cdot n$ операцій віднімання для

формування значень δ та $2 \cdot n$ операцій додавання при формуванні кінцевого результату. Таким чином, числове значення часу, який витрачається для здійснення операції дискретного перетворення Фур'є за запропонованою процедурою на обчислювальній платформі користувача – T_K визначається за наступною формулою:

$$T_к = 4 \cdot n \cdot t_a . \qquad (2.21)$$

Відповідно, коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є визнається наступною формулою:

$$\nu = \frac{T_Б}{T_K} = \frac{(31 \cdot n^2 - n) \cdot t_a}{4 \cdot n \cdot t_a} \approx 7 \cdot n . \qquad (2.22)$$

Наприклад, для n=8 числове значення коефіцієнту ν прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є обчислений за формулою (2.22) становить коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є складає ν=56, а при n=128 коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу складає ν=896.

При виборі в якості базового варіант виконання дискретного перетворення Фур'є в формі швидкого перетворення Фур'є, коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу захищеного дискретного перетворення Фур'є на віддалених обчислювальних потужностях визнається наступною формулою:

$$\nu' = \frac{T'_Б}{T_K} = \frac{31 \cdot n^2 \cdot t_a}{8 \cdot n \cdot t_a} \approx 4 \cdot n . \qquad (2.23)$$

Наприклад, при n=8 числове значення коефіцієнту ν′ прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є обчислений за формулою (2.23)

складає ν=32, а при n=128 коефіцієнт ν′ прискорення обчислень за рахунок використання запропонованого методу становить ν′=512.

З цього можна зробити два важливих висновки:

- Використання віддалених багатопроцесорних обчислювальних систем для прискорення обчислювальної реалізації дискретного перетворення Фур'є дає значний ефект в плані прискорення виконання обчислень, що дуже важливо для практичних застосувань, що функціонують в режимі реального часу;

- ефективність використання в рамках хмарних технологій віддалених багатопроцесорних обчислювальних систем для прискорення обчислювальної реалізації дискретного перетворення Фур'є лінійно зростає зі збільшенням значення розмірності перетворення - n.

Як зазначалося вище, рівень захищеності розроблено методу визначається здатністю зловмисника, що має доступ до віддаленої комп'ютерної системи, на якій виконується дискретне перетворення Фур'є над даними користувача або до каналу обміну, відновити значення відліків сигналу X. Для цього йому потрібно знати вибраний для шифрування корисного сигналу X опорний сигнал B. Якщо для кожного віддаленого дискретне перетворення Фур'є використовується свій опорний сигнал, то, у відповідності з криптографічним принципом К. Шеннона [18] це зробити в принципі не можливо. Проте зрозуміло, що на практиці використання спеціального опорного сигналу для кожного корисного сигналу X не має сенсу з точки зору виграшу в часі виконання дискретного перетворення Фур'є. Тому, реально, кількість χ опорних сигналів обмежена.

Якщо для захисту двох сигналів X та X′ використовувався один і той же опорний сигнал B, то зловмисних не зможе виявити цей факт, не знаючи цих сигналів. Для того, щоб отримати шанс реалізувати незаконний доступ до сигналів користувача, які оброблюються на віддаленій системі, зловмисник має знати деяку підмножину Δ вхідних сигналів. Тоді він може відновити

підмножину опорних сигналів. які використовувалися користувачем для організації захищеної обробки вхідних сигналів множини Δ. Зокрема, якщо зловмисник за якимись іншими каналами отримав сигнал X′, то він може сформувати значення відліків цього сигналу: x_0', x_1',…, x_{n-1}' і, маючи у своє розпорядженні надіслані в систему відліки δ_0',δ_1',…,δ_{n-1}' має змогу відновити відліки опорного сигналу за такою формулою:

$$\forall i \in \{0,1,2,...,n-1\} : B_{qi} = \delta_i' - x_i' . \qquad (2.24)$$

Цілком очевидно, що ймовірність p_0 того, що за вказаним сценарієм зловмиснику пощастить успішно дешифрувати сигнал, поданий у вигляді набору зміщень δ_0,δ_1,…,δ_{n-1} відносно невідомого опорного сигналу дорівнює $p_0 = \psi/\chi$, де ψ - кількість опорних сигналів, які складають множину Δ відомих зловмиснику опорних сигналів користувача.

2.3 Розробка способу захищеної реалізації перетворення Фур'є адитивного розкладенням на складові відліків сигналу

Ще одна можність організації захищеного виконання дискретного перетворення Фур'є на віддалених обчислювальних потужностях полягає в тому, щоб кожен з відліків сигналу X розкласти на *k* адитивних складових.

В рамках реалізації цієї ідеї пропонується при віддаленій обробці сигналу X, який задається *n* відліками x_0,x_1,…,x_{n-1} довільним чином вибрати *n* *k*-бітових ключів D_0,D_1,…,D_{n-1}, кожен з яких використовується для адитивного шифрування відповідного з відліків x_0,x_1,…,x_{n-1} .

Будь-який *j*-ключ D_j, $j \in \{0,1,2,…,n-1\}$, може бути представлений у вигляді: $D_j = d_{j0} + d_{j1}\cdot 2 + d_{j2}\cdot 2^2 + … + d_{j(n-1)}\cdot 2^{n-1}$, де d_{j0},d_{j1},…,$d_{j(n-1)} \in \{0,1\}$. Тоді j–тій відлік сигналу X – x_j може бути представлений у наступному вигляді:

$$\forall j \in \{0,1,...,n-1\} : x_j = \sum_{i=0}^{n-1} (2 \cdot d_{ji} - 1) \cdot g_{ji} . \qquad (2.25)$$

Відповідно, користувач надсилає в віддалену систему *n* наборів: перший набір: g_{00},g_{01},…,$g_{0(n-1)}$, другий набір: g_{10},g_{11},…,$g_{1(n-1)}$ і так далі до останнього:

$g_{(n-1)0}, g_{(n-1)1}, \ldots, g_{(n-1)(n-1)}$. Над з кожним j-тим з цих n наборів чисел віддалена комп'ютерна система виконує дискретне перетворення Фур'є:

$$\forall i \in \{0,1,...,n-1\} : y_{ji} = \frac{1}{n}\sum_{l=0}^{n-1} g_{ji} \cdot a_{il},$$
$$z_{ji} = \frac{1}{n}\sum_{l=0}^{n-1} g_{jl} \cdot c_{il} \qquad (2.26)$$

Відповідно, віддалена комп'ютерна система повертає користувачеві $2 \cdot n$ наборів чисел. Перші два набори з них являють собою реальну $y_{01}, y_{02}, \ldots, y_{0(n-1)}$ і уявну $z_{01}, z_{02}, \ldots, z_{0(n-1)}$ частини спектру відліків $g_{00}, g_{01}, \ldots, g_{0(n-1)}$, друга пара наборів чисел $y_{11}, y_{12}, \ldots, y_{1(n-1)}$ і $z_{11}, z_{12}, \ldots, z_{1(n-1)}$ являють собою набір значень відповідно, реальних компонент і уявних компонент спектрального представлення відліків $g_{10}, g_{11}, \ldots, g_{1(n-1)}$. Тобто, кожна j-та пара наборів чисел що повертаються системою: $y_{j1}, y_{j2}, \ldots, y_{j(n-1)}$ і $z_{j1}, z_{j2}, \ldots, z_{j(n-1)}$ являють собою набір значень відповідно, реальних компонент і уявних компонент спектрального представлення j-тої групи відліків $g_{j0}, g_{j1}, \ldots, g_{j(n-1)}$.

Користувач відновлює значення $(n\text{-}1)$ реальних компонент $r_0, r_1, \ldots, r_{n-1}$ спектру сигналу X, так, що кожна j-та з них формується як сума всіх j-тих реальних компонент спектрів $g_{00}, g_{01}, \ldots, g_{0(n-1)}, \ldots, g_{(n-1)0}, g_{(n-1)1}, \ldots, g_{(n-1)(n-1)}$ за наступною формулою:

$$\forall j \in \{0,1,...,n-1\} : r_j = \sum_{l=0}^{n-1} (2 \cdot d_l - 1) \cdot y_{lj} \ . \qquad (2.27)$$

Аналогічно, користувач формує значення $(n\text{-}1)$ уявних компонент $m_0, m_1, \ldots, m_{n-1}$ спектру сигналу X у вигляді суми одноіменних уявних компонентів $z_{00}, z_{01}, \ldots, z_{0(n-1)}, \ldots, z_{(n-1)0}, z_{(n-1)1}, \ldots, z_{(n-1)(n-1)}$ спектрів відліків $g_{00}, g_{01}, \ldots, g_{0(n-1)}, \ldots, g_{(n-1)0}, g_{(n-1)1}, \ldots, g_{(n-1)(n-1)}$ згідно з наступною формулою:

$$\forall j \in \{0,1,...,n-1\} : m_j = \sum_{l=0}^{n-1} (2 \cdot d_l - 1) \cdot z_{lj} \qquad (2.28)$$

Коректність наведених перетворень може бути доведена наступним чином. Якщо в формулу (2.27) підставити значення y_{ij} з формули (2.26) то вона формула трансформується до наступного виду:

$$\forall j \in \{0,1,...,n-1\} : r_j = \sum_{l=1}^{m-1} (2 \cdot d_l - 1) \cdot \sum_{h=0}^{n-1} g_{lh} \cdot a_{jh} \ . \qquad (2.29)$$

Оскільки $(2 \cdot d_l\text{-}1)$ не залежить від індексу h другої суми, цей фрагмент можна внести до другої суми:

$$\forall j \in \{0,1,...,n-1\} : r_j = \sum_{l=1}^{m-1} \sum_{h=0}^{n-1} (2 \cdot d_l - 1) \cdot g_{lh} \cdot a_{jh} \ . \qquad (2.30)$$

Порядок обчислення сум в формулі (2.30) може бути змінений:

$$\forall j \in \{0,1,..,n-1\} : r_j = \sum_{h=0}^{n-1} \sum_{l=1}^{m-1} (2 \cdot d_l - 1) \cdot g_{lh} \cdot a_{jh} \ . \qquad (2.31)$$

Оскільки a_{jh} не залежить від індексу l, то a_{jh} можна винести за межі другої суми. В результаті цього формула (2.31) трансформується до вигляду:

$$\forall j \in \{0,1,..,n-1\} : r_j = \sum_{h=0}^{n-1} a_{jh} \cdot \sum_{l=1}^{m-1} (2 \cdot d_l - 1) \cdot g_{lh} \ . \qquad (2.32)$$

Значення другої суми в виразі (2.32) може бути представлене у відповідності з формулою (2.25) наступним чином:

$$\sum_{l=1}^{b-1} (2 \cdot d_l - 1) \cdot g_{lh} = x_h \ . \qquad (2.33)$$

Підстановка заміни (2.33) в формулу (2.32) трансформує її до такого вигляду:

$$\forall j \in \{0,1,..,n-1\} : r_j = \sum_{h=0}^{n-1} a_{jh} \cdot x_h \ . \qquad (2.34)$$

Отриманий вираз (2.34) співпадає з виразом (2.4) для отримання реальних компонентів спектру сигналу X. Це означає, що запропоновані перетворення забезпечують отримання коректного результату.

Аналогічно, в формулі (2.28) можна замінити значення u_{ij} її представленням формулою (2.26). Відповідно, формула (2.28) трансформується до наступного виду:

$$\forall j \in \{0,1,...,n-1\} : m_j = \sum_{l=1}^{m-1} (2 \cdot d_l - 1) \cdot \sum_{h=0}^{n-1} g_{lh} \cdot c_{jh} \ . \qquad (2.35)$$

Оскільки ($2 \cdot d_l$-1) не залежить від індексу h другої суми, цей фрагмент може бути внесений до другої суми в формулі (2.35), що трансформує її до такого вигляду :

$$\forall j \in \{0,1,...,n-1\} : m_j = \sum_{l=1}^{m-1} \sum_{h=0}^{n-1} (2 \cdot d_l - 1) \cdot g_{lh} \cdot c_{jh} . \qquad (2.36)$$

Порядок обчислення сум в формулі (2.36) може бути змінений:

$$\forall j \in \{0,1,..,n-1\} : m_j = \sum_{h=0}^{n-1} \sum_{l=1}^{m-1} (2 \cdot d_l - 1) \cdot g_{lh} \cdot c_{jh} . \qquad (2.37)$$

Оскільки коефіцієнт c_{jh} не залежить від індексу l, то його можна винести за межі другої суми. В результаті цього формула (2.37) трансформується до вигляду:

$$\forall j \in \{0,1,..,n-1\} : m_j = \sum_{h=0}^{n-1} c_{jh} \cdot \sum_{l=1}^{m-1} (2 \cdot d_l - 1) \cdot g_{lh} . \qquad (2.38)$$

Значення другої суми в виразі (2.38) може бути представлене у відповідності з формулою (2.25) наступним чином:

$$\sum_{l=1}^{b-1} (2 \cdot d_l - 1) \cdot g_{lh} = x_h . \qquad (2.39)$$

Підстановка заміни виразу для другої суми (2.39) в формулу (2.38) трансформує її до наступного вигляду:

$$\forall j \in \{0,1,..,n-1\} : m_j = \sum_{h=0}^{n-1} c_{jh} \cdot x_h . \qquad (2.40)$$

Отриманий вираз (2.40) співпадає з виразом (2.4) для отримання уявних компонентів спектру сигналу X. Це означає, що запропоновані перетворення забезпечують отримання коректного результату і для уявних компонент спектру сигналу X.

Оцінка ефективності включає визначення значення двох критеріїв:

- рівень захищеності від спроб незаконного доступу до відліків сигналів, який визначається об'ємом ресурсів, необхідних для відновлення зловмиснику відліків реального сигналу X.

- коефіцієнтом ν прискорення обчислювальної реалізації дискретного перетворення Фур'є, який визначається формулою (2.17). В цій формулі фігурує значення $T_Б$ – часу обчислень в базовому варіанті –тобто згідно формул (2.1) та час T_K обчислень, пов'язаних з виконанням дискретного перетворення Фур'є за запропонованим методом, тобто часу, який витрачається для здійснення цієї операції на обчислювальній платформі користувача.

Час виконання перетворень Фур'є в базовому варіанті реалізації дискретного перетворення Фур'є на обчислювальній платформі користувача визначається формулою (2.18) чи її конкретизацією у вигляді (2.19).

Як зазначалося вище, в практиці цифрової обробки сигналів дискретне перетворення Фур'є часто реалізується в формі швидкого перетворення Фур'є, що дозволяє практично вдвоє зменшити кількість операцій множення та додавання за рахунок використання властивостей симетрії коефіцієнтів дискретне перетворення Фур'є. При застосуванні швидкого перетворення Фур'є $T_Б'$ виконання перетворення визначається формулою (2.20).

При використання запропонованого методу, на обчислювальній платформі користувача виконується тільки $k{\cdot}n$ операцій додавання для формування значень наборів, які посилаються на віддалену систему і $k{\cdot}n$ операцій додавання при формуванні кінцевого результату. Таким чином, числове значення часу, який витрачається для здійснення операції дискретного перетворення Фур'є за запропонованою процедурою на обчислювальній платформі користувача – T_K визначається за наступною формулою:

$$T_к = 2 \cdot k \cdot n \cdot t_a . \qquad (2.41)$$

Відповідно, коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є визнається наступною формулою:

$$\nu = \frac{T_Б}{T_K} = \frac{(31 \cdot n^2 - n) \cdot t_a}{2 \cdot k \cdot n \cdot t_a} \approx \frac{15 \cdot n}{k}. \qquad (2.42)$$

Наприклад, для n=8 і k=4 числове значення коефіцієнту ν прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є обчислений за формулою (2.42) становить складає ν=30, а при n=128 коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу складає ν=480.

При виборі в якості базового варіант виконання дискретного перетворення Фур'є в формі швидкого перетворення Фур'є, коефіцієнт ν прискорення обчислень за рахунок використання запропонованого методу захищеного дискретного перетворення Фур'є на віддалених обчислювальних потужностях визнається наступною формулою:

$$\nu' = \frac{T'_Б}{T_K} = \frac{31 \cdot n^2 \cdot t_a}{4 \cdot k \cdot n \cdot t_a} \approx \frac{8 \cdot n}{k}. \qquad (2.43)$$

Наприклад, при n=8 та k=4 числове значення коефіцієнту ν′ прискорення обчислень за рахунок використання запропонованого методу віддаленого захищеного дискретного перетворення Фур'є обчислений за формулою (2.43) складає ν=16, а при n=128 коефіцієнт ν′ прискорення обчислень за рахунок використання запропонованого методу становить ν′=256.

З цього можна зробити два важливих висновки:

- Використання віддалених багатопроцесорних обчислювальних систем для прискорення обчислювальної реалізації дискретного перетворення Фур'є дає значний ефект в плані прискорення виконання обчислень, що дуже важливо для практичних застосувань, що функціонують в режимі реального часу;

- ефективність використання в рамках хмарних технологій віддалених багатопроцесорних обчислювальних систем для прискорення обчислювальної реалізації дискретного перетворення Фур'є лінійно зростає зі збільшенням значення розмірності перетворення - n.

Недоліком описаної технології організації віддаленого обчислення в хмарі є той факт, що знайдена підпослідовність може бути занадто великою (наприклад, показник складається з двох ідентичних частин). В такому випадку значно ускладнюється процес розпаралелювання обчислень, який починає обмежуватись не кількістю доступних вузлів хмарної системи, а кількістю груп, на які вдалося розбити показник.

Як зазначалося вище, рівень захищеності розроблено методу визначається здатністю зловмисника, що має доступ до віддаленої комп'ютерної системи, на якій виконується дискретне перетворення Фур'є над даними користувача або до каналу обміну, відновити значення відліків сигналу X.

Для того, щоб зловмисник міг відновити значення відліків $x_0,x_1,\ldots,x_{n-1}$ корисного сигналу X по системі n наборів, які передаються користувачем в систему: перший набір: $g_{00},g_{01},\ldots,g_{0(n-1)}$, другий набір: $g_{10},g_{11},\ldots,g_{1(n-1)}$ і так далі до останнього: $g_{(n-1)0},g_{(n-1)1},\ldots,g_{(n-1)(n-1)}$ йому потрібно перебрати всі можливі значення коефіцієнтів d.

При використанні розробленого методу кількість E можливих перестановок коефіцієнтів дорівнює $k!$, що, за формулою Стірлінга, наближено становить:

$$E = (\frac{k}{e})^k \cdot \sqrt{2 \cdot \pi \cdot k} . \qquad (2.43)$$

Для реальних сигналів найменша кількість k складає 32, відповідно, мінімальна кількість варіантів перестановок стовбців становить $8.56 \cdot 10^{34}$. Це практично унеможливлює відновлення оригінального сигналу користувача шляхом підбору зворотної перестановки, оскільки перебір такої кількості варіантів виходить за рамки можливостей технічної реалізації.

Для певних класів сигналів об'єм перебору може бути суттєвим чином зменшено за рахунок направленої його реконструкції. Ця технологія передбачає вибір коефіцієнтів таким чином , щоб два сусідніх мінімально відрізнялись один від одного. Проведені експериментальні дослідження

показали, що для реальних сигналів об'єм перебору може бути зменшено на порядки.

Виходом з такої ситуації може бути введення додаткового обмеження – пошук найбільшого підрядка, що повторюється, довжиною не більше заданого числа k біт. В такому випадку, знаючи кількість n наявних вузлів хмарного обчислювача та довжину n показника, значення δ встановлюється як $\delta = k/n$, що буде гарантувати завантаження всіх наявних ресурсів.

При захищеній обробці сигналів цих класів з використанням розробленого методу рекомендується організовувати одночасну обробку групи з n сигналів. При цьому відліки сигналів перемішуються в межах групи. Кількість сигналів в межах однієї групи не впливає на час виконання шифрування та дешифрування, а також не змінює об'єм пам'яті необхідний для збереження секретних ключів. Проте кількість варіантів перестановок збільшується, що суттєво підвищує рівень захищеності реалізації дискетного перетворення Фур'є.

При практичній реалізації запропонованого методу захищеного виконання дискретного перетворення Фур'є на віддалених комп'ютерних системах важливим питання є вибір значень n наборів: від першого набору: $g_{00},g_{01},\ldots,g_{0(n-1)}$, другого набору: $g_{10},g_{11},\ldots,g_{1(n-1)}$ і так далі до останнього набору: $g_{(n-1)0},g_{(n-1)1},\ldots,g_{(n-1)(n-1)}$.

Для розв'язання цієї задачі пропонується використати такі структури даних, як суфіксні дерева та суфіксний масив.

Суфіксне дерево T для набору чисел довжини n - це орієнтоване дерево, що має n листів пронумерованих від 1 до n. Кожна вершина, крім кореня дерева, має щонайменше два відгалуження. Кожне ребро суфіксного дерева марковане непорожнім підрядком E рядка S. Жодна вершина не може мати ребра, які починаються з однакового номеру. Важливою властивістю такого дерева є те, що конкатенація номерів ребер на шляху від кореня до термінальної вершини формує значення числа для вказаних вище наборів.

Використання описаної технології з застосуванням суффіксних дерев дозволяє розв'язувати за лінійний час задачу генерації ефективних в плані захисту наборів даних.

Тривіальним способом побудови суффіксного дерева видається знаходження списку всіх суфиксів з подальшим його впорядкуванням. Такий підхід дозволяє побудувати дерево з використанням $O(n \cdot \log_2 n)$ операцій, оскільки для сортувань, заснованих на порівнянні (*comparison-based sortings*) саме є теоретичним мінімумом.

Проте, існують набагато більш ефективні алгоритми побудови суффіксного дерева [19]. Маючи готове суффіксне дерево, можна побудувати масив чисел для адитивного маскування відліків за лінійний час. Суффіксне дерево також може бути побудовано за лінійний час (наприклад, використовуючи алгоритм Укконена) [19].

В результаті виконаних досліджень, досягнута поставлена ціль – розроблено оригінальний метод захищеної реалізації дискретного перетворення Фур'є на віддалених обчислювальних потужностях в рамках хмарних технологій.

Запропонований метод, по суті, реалізує адитивне шифрування відліків сигналів користувача.

Головна перевага запропонованого методу полягає в простоті операцій шифрування відліків корисного сигналу X та дешифрування отриманих від системи даних для реконструкції спектру сигналу даних, що забезпечує низький рівень витрат обчислювального часу на виконання операцій, пов'язаних з захистом інформації.

Теоретично доведено, що запропонований метод захищеної реалізації потоку операцій ДПФ забезпечує достатній для задач практики рівень захищеності даних та результатів перетворення Фур'є, що виконуються на віддалених обчислювальних потужностях та передаються по відкритим каналам Інтернет.

Теоретично та експериментально доведено, що використання запропонованого методу забезпечує підвищення швидкості обробки зображень та звукових сигналів на 3-4 порядки.

Розроблений метод може бути ефективно використаний для потокової обробки зображень в реальному часі, зокрема, в системах обробки супутникових зображень, а також в інтелектуальних системах відеоспостереження.

Запропонований метод, що полягає в використанні адитивних масок може бути модифіковано для закритого обчислення швидкого перетворення Фурє на віддалених обчислювальних потужностях.

Висновки до розділу 2

В результаті виконання досліджень, направлених на розробку організації захищеного виконання дискретного перетворення Фур'є на віддалених обчислювальних потужностях в рамках хмарних технологій отримані наступні результати:

1. Теоретично досліджено організацію обчислень, які складають дискретне перетворення Фур'є в плані виявлення можливостей його захищеної реалізації на віддалених і неконтрольованих комп'ютерних системах. Показано, що характер обчислень виключає можливість використання підстановочних шифрів та шифрів, основаних на мультиплікативних операціях. Аналіз показав малу ефективність переходу для реалізації функцій захисту в інші алгебраїчні базиси. Найбільш перспективною формою шифрів для захисту даних під час віддаленої реалізації дискретного перетворення Фур'є є використання різних різновидів адитивних шифрів.

1. Теоретично обґрунтовано, розроблено та експериментально досліджено метод захищеної реалізації дискретного перетворення Фур'є на віддалених багатопроцесорних комп'ютерних системах, відмінністю якого є використання опорних значень для адитивного маскування відліків сигналів перед їх передачею на віддалені комп'ютерні системи. Теоретично та експериментально доведено, що запропонований метод дозволяє на 2-3 порядки прискорити цифрову обробку сигналів за рахунок розпаралелювання обчислень на віддалених багатопроцесорних системах. Детально розроблено технологію практичного застосування запропонованого методу захищеної реалізації дискретного перетворення Фур'є на віддалених багатопроцесорних комп'ютерних системах

3. Розроблено та досліджено метод захищеної реалізації перетворення Фур'є з адитивним розкладенням на складові відліків сигналу. Метод забезпечує безпечну операцію дискретного перетворення Фур'є на віддалених

комп’ютерних системах в рамках хмарних технологій. Теоретичними обрахунками та експериментально доведено, що запропонований метод дозволяє на 2-3 порядки прискорити цифрову обробку сигналів за рахунок розпаралелювання обчислень на віддалених багатопроцесорних системах. Детально розроблено методику застосування запропонованого методу для дискретного перетворення Фур’є, теоретично доведено конструктивність розроблених процедур. Теоретично доведено, що запропонований метод захищеної реалізації дискретного перетворення Фур’є забезпечує достатній для задач практики рівень захищеності даних.

РОЗДІЛ 3
РОЗРОБКА ПРОГРАМНИХ ЗАСОБІВ ДЛЯ РЕАЛІЗАЦІЇ МЕТОДУ ЗАХИЩЕНОЇ РЕАЛІЗАЦІЇ ПЕРЕТВОРЕННЯ ФУР'Є

Для сучасного етапу розвитку інформаційних та комп'ютерних технологій характерним є динамічне розширення інтерфейсу між зовнішнім світом та засобами комп'ютерної обробки інформації. Домінуючу роль у цьому процесі відіграють засоби цифрової обробки сигналів, в основі яких лежить дискретне перетворення Фур'є. Цей чинник сприяє розширенню кола застосування дискретного перетворення Фур'є. Зростають і вимоги до якості перетворення.

Потужний імпульс розширенню використання дискретного перетворення Фур'є надає розповсюдження систем відео нагляду. Ці системи широко використовуються в технологічних процесах, системах регулювання, а також, є технологічною основою боротьби з проявами тероризму. Характерним для таких систем є те, що вони працюють в середовищі Інтернет у реальному часі, а це, в свою чергу, диктує жорсткі вимоги до швидкості реалізації дискретного перетворення Фур'є.

Важливою складовою розробки методу захищеної реалізації операцій, пов'язаних з дискретним перетворенням Фур'є на віддалених комп'ютерних системах є експериментальна перевірка отриманих результатів.

В рамках експериментальних досліджень потрібно перевірити на практиці коректність результатів обчислень, а також практична перевірка працездатності запропонованого методу захищеного обчислення дискретного перетворення Фур'є в критичних режимах роботи. Крім того, експериментальні дослідження мають практично оцінити досягнутий виграш у часі реалізації дискретного перетворення Фур'є за рахунок залучення віддалених обчислювальних потужностей, з можливістю паралельної реалізації процесу. З використанням експериментальних досліджень можна отримати залежність коефіцієнту прискорення дискретного перетворення

Фур'є від кількості відліків сигналу X та порівняти отримані результати цієї залежності з отриманими теоретичним шляхом.

Для виконання означених вище експериментальних досліджень запропонованого методу захищеної реалізації дискретного перетворення Фур'є на віддалених комп'ютерних системах розроблена програма моделювання обчислень. Програма виконана на мові програмування C++ в середовищі Visual Studio 2010.

3.1 Опис структурної організації даних

Сучасні інтеграційні шляхи розвитку обчислювальної техніки, зумовили низько-апаратну реалізацію більшості операції роботи з вбудованими типами в мовах програмування [11]. Так, цілочисельний тип Integer має розрядність 32 біта або 64 біта в залежності від розрядності процесора обчислювальної платформи, що дозволяє виконувати арифметичні операції на апаратному рівні. Робота з чисельними типами, розрядність яких перевищує розрядність процесора, базується на ідеї представлення цих чисел в двійковій системі і використання бітових рядків або масивів. Кожен елемент масиву в такій інтерпретації співвідноситься з розрядності процесора і містить в собі частину бітів багаторозрядного числа.

В виконаній в рамках дипломного проекту розробки використовуються числа з плаваючою точкою. Це диктується тим, що дискретне перетворення Фур'є використовується на практиці над реальними числами, які представляють відліки аналогового сигналу X і отримуються як результат дискретизації цього сигналу по часу та по значенню. Тому, в розробленій програмі використовуються числа з плаваючою точкою.

Для представлення сукупності вимірів, проміжних даних та результатів використовується масив з *n* чисел типу float. В таких массивах розміщуються дані про відліки сигналу X користувача, дані про зашифровані відліки, які безпосередньо надсилаються користувачем в систему, результати віддаленої обробки зашифрованих відліків, які повертаються системою користувачеві в

якості результату. В форматі вказаного масиву розміщуються дані, над якими здійснюється дешифрування, тобто відновлення коректного результату дискретного перетворення Фур'є. Описана організація даних значно спрощує операцію вибірки елементів масиву, що впливає на швидкодію роботи.

В першому з розроблених у другому розділі методів для шифрування використовуються опорні значення відліків та відповідні їм результати дискретного перетворення Фур'є у вигляді реальної та уявної компонент. Ці значення зберігаються в програмі у вигляді двовимірного масиву, рядками якого номери опорних значень, а трьома стовпчиками – відповідно значення опорні значення відліків та відповідні їм результати дискретного перетворення Фур'є у вигляді реальної та уявної компонент. Звернення до такого масиву опорних значень організовано через систему вказівників, які змінюються на величину розміру масиву опорних відліків.

При моделюванні віддаленої обробки зашифрованих відліків сигналу користувача на багатопроцесорних комп'ютерних системах використовується попереднє обчислення коефіцієнтів дискретного перетворення Фурє. До формул (2.1) дискретного перетворення Фур'є входять компоненти, які не залежать від значень відліків $x_0, x_2, \ldots x_{n-1}$ і їх можна вважати постійними числами, значення яких визначаються лише індексами. Тому, попередньо в розробленій програмі обчислюються складові формул (2.1) у вигляді набору коефіцієнтів, які, в подальших дослідженнях можуть вважатися постійними і зберігаються в двох двовимірних масивах A і C, які містять числа з плаваючою точкою, обчислені спеціальною процедурою згідно з формулам (2.3).

Очевидно, що елементи цих двох двовимірних масивів чисел з плаваючою точкою е симетричними відносно головної діагоналі. Це означає, що існує теоретична можливість використання більш складної структури для зберігання постійних коефіцієнтів, що використовуються для формування реального та уявних компонентів спектру заданого сигналу. Властивість симетрії цих коефіцієнтів широкого використовується у вигляді модифікації процедури дискретного перетворення Фур'є у вигляді широко відомого

алгоритмі швидкого перетворення Фур'є. Проте проведений аналіз показав, що використання складних структур для збереження масивів коефіцієнтів дискретного перетворення Фур'є недоцільне виходячи з того, що це помітно ускладнить звернення до даних, знизить рівень надійності програмного забезпечення та суттєво уповільнить виконання програми.

3.2 Розробка програмних модулів

В розробленій програмі реалізовано обидва описані в другому розділі проекту методи захищеної реалізації дискретного перетворення Фур'є на віддалених комп'ютерних системах.

В першому методі для шифрування використовуються опорні значення відліків та відповідні їм результати дискретного перетворення Фур'є у вигляді реальної та уявної компонент. Ці данні розраховуються спеціальним модулем, а в реальності здійснюються користувачем на етапі підготовки до віддаленої роботи. Фактично, ці опорні значення відліків відіграють роль секретних ключів користувача і мають зберігатися в спеціально захищеній пам'яті, або в зашифрованому вигляді. Шифрування здійснюється в використанням симетричних шифрів типу DES або AES. Розшифровування опорного блоку виконується безпосередньо перед його використанням.

В другому методі розроблена спеціальна процедура для генерації випадкових значень. В процедурі випадковим чином генерується χ-1 відлік, а останній відлік утворюється таким чином, щоб його сума з усіми згенерованими дорівнювала реальному значенню відліку. Крім того, випадковим чином генерується значення знаку (плюс чи мінус) з яким в сумі враховується випадково згенероване значення відліку. Для того, щою статистичними методами неможливо було відсіяти вплив випадково згенерованих компонентів, вини генеруються близькими в заданих межах до реального відліку. Для цього в розробленій процедури для заданого відліками сигналу користувача X визначається діапазон їх змін, як різниця між максимальним та мінімальним значень відліку. Відповідно, генерація випадкових складових, які маскують корисний сигнал при його віддаленому

перетворенні Фур'є здійснюється тільки у визначеному діапазоні. Для цього спочатку з використанням вбудованого генератора C++ генерується float число в діапазоні від нуля до одиниці, а потім воно множиться на величину діапазону з додавання нижньої границі діапазону.

Класи Coder та Decoder відповідають за гомомогенне шифрування відліків сигналу користувача да декодування отриманої від віддаленої системи результатів з метою реконструкції коректного результату дискретного перетворення Фурє. Для кодування та виправлення масивів чисел з плаваючою точкою ці класи створюють об’єкти класу.

На етапі проектування інтерфейсу програми було створено три класи та чотири допоміжнімфайли FXML графічного інтерфейсу. “ParametersWindow” — файл графічного інтерфейсу, який включає в себе поля для вводу вхідних параметрів, та кнопку початку моделювання гомомогенного шифрування даних користувача, зображення кроків роботи програми від початку шифрування відліків, до дешифрування користувачем отриманих від віддаленої системи результатів дискретного перетворення Фур'є. “ParametersRootLayout” — файл графічного інтерфейсу, який відіграє роль обгортки для елементів файлу графічного інтерфейсу “ParametersWindow”. “GeneralViewWindow” — файл графічного інтерфейсу, який включає в себе елементи графічного інтерфейсу для зображення етапів моделювання шифрування, віддаленої обробки та дешифрування результату, поля для вводу вхідних параметрів, та кнопку переходу до наступного кроку моделювання. “GeneralViewRootLayout” — файл графічного інтерфейсу, який виступає у ролі обгортки для елементів файлу графічного інтерфейсу “GeneralViewWindow”. “ParametersWindowController” — клас, який виступає у ролі контролера для елементів файлу графічного інтерфейсу “ParametersWindow”. Цей клас реалізую функціонал кнопки, полів та перевірку коректності введених даних в ці поля. “GeneralViewWindowController” — клас, який виступає у ролі контролера для

елементів файлу графічного інтерфейсу “GeneralViewWindow”. Цей клас реалізує функціонал кнопок, полів та перевірку коректності введених даних в ці поля. Крім того, описаний клас реалізує методи для графічного відображення кроків моделювання етапів гомомогенного шифрування відліків сигналу користувача, віддаленої обробки зашифрованих відліків, а також відновлення коректного результату дискретного перетворення Фур’є. “MainApp” — головний клас розробленого модуля інтерфейсу, який використовується для запуску програми в режимах дослідження та моделювання, а також використовується в ролі проміжної ланки між класами контролерами графічних інтерфейсів.

ВИСНОВКИ ДО РОЗДІЛУ 3

В результаті виконання розробок, які складають третій розділ дипломного проекту, і мають на меті створення програмного забезпечення для експериментальної перевірки та моделювання запропонованого методу захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах можна зробити такі висновки:

1. Розроблено програмні засоби моделювання методу захищеної реалізації дискретного перетворення Фур'є на віддалених багатопроцесорних комп'ютерних системах, відмінністю якого є використання опорних значень для адитивного маскування відліків сигналів перед їх передачею на віддалені комп'ютерні системи. З використанням розроблених програмних засобів проведено перевірку функціональної коректності запропонованого методу, підтверджено його працездатність, а також експериментально, з використанням технологій статистичного моделювання показано, що розроблений метод дозволяє на 2-3 порядки прискорити цифрову обробку сигналів за рахунок розпаралелювання обчислень на віддалених багатопроцесорних системах. Довжина ключа дорівнює s·n бітів, що становить близько 2^{10}, тобто для його підбору потрібно виконати 2^{1024} перебори, що виходить за рамки технічних можливостей сучасних комп'ютерних систем і достатньо надійно гарантує захист даних користувача при ї віддалений обробці на неконтрольованих обчислювальних платформах.

2. Розроблено готові до практичного використання програмні засоби, які реалізують метод захищеної реалізації перетворення Фур'є з адитивним розкладенням на складові відліків сигналу. З використанням розроблених програмних засобів здійснено перевірку функціональної коректності розробленого методу, підтверджено його працездатність на всіх режимах роботи. З використанням створених програмних засобів, експериментально, з використанням технологій статистичного моделювання показано, що цей метод метод дозволяє на 2 порядки прискорити цифрову обробку сигналів і

забезпечує високий рівень захисту за рахунок того, що блокує спроби незаконної реконструкції відліків сигналу методами статистичного аналізу. Велика довжина ключа практично виключає методи злому захисту з використанням перебору.

Список використаної літератури

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Markovskyi O.P. Secure Modular Exponentiation in Cloud Systems/ O.P. Markovskyi, N. Bardis, S.J. Kirilenko // Proceeding of the Congress on Information Technology. Computationnal and Experimental Physics (CITCEP 2015), 18-20 December 2015, Krakow. Poland. – PP.266-269.
2. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing/ N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – Issue 4. – 2012. – №3. – PP. 169-180.
3. Bos J.N. Additional chain heuristics / J.N. Bos, M. Coster // Cryptographic Hardware and Embedded System- CHES'2014. LNCS-2116, Springer-Verlag. – 2014. – P.143-151.
4. Марковський О.П. Захищена реалізація фільтрації зображень в GRID-системах / О.П. Марковський, М.В. Невдащенко, А.М. Білашевська // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка. – Київ: ВЕК+. – 2014. – № 61. – С.105-109.
5. Костенко Ю. В. Метод защищенного модулярного экспоненцирования на удаленных компьютерных системах / Ю. В. Костенко, А.П. Марковский, О.В. Русанова // Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+". – № 64. – 2016. – С. 51-54.
6. Буйбарова М.Ф. Метод захищеної реалізації перетворень Фур'є на віддалених розподілених комп'ютерних системах / М.Ф. Буйбарова, Ю.М. Виноградов, В.Ю. Приймак // Вісник Національного технічного

університету України “КПІ” Інформатика, управління та обчислювальна техніка. – К.: ТОО „ВЕК+”. – № 64. – 2016. – С. 64-71.

7. Вельшенбах М. Криптография на С и С++ в действии / М. Вельшенбах. – М.: Триумф. – 2004. – 460 с.
8. Гамаюн В.П. Квазиграфический метод вычисления остатка по модулю / В.П. Гамаюн //Проблеми інформатизації та управління. Зб.наукових праць. – К.: НАУ. – 2005. – Вип.3(14). – С.43-48.
9. Домашнев А.В. Программирование алгоритмов защиты информации / А.В. Домашнев, М.М. Грунтович, В.О. Попов, Д.И. Правиков, А.Ю. Щербаков, И.В. Прокофьев. – М.: Нолидж. – 2002. – 409 с.
10. ДСТУ 3396.0=96. Захист інформації. Технічний захист інформації. Основні положення. – К.: Держстандарт України. – 1997. – 14 с.
11. Анісімов А.В. Алгоритмічна теорія великих чисел / А.В. Анісімов. – К.: Академперіодика. – 2001. – 153 с.
12. ДСТУ 3396.2-96. Захист інформації. Технічний захист інформації. Терміни та визначення. – К.: Держстандарт України. – 1997. – 11 с.
13. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу. НД ТЗІ 2.5-004-99.
14. Задірака В.К. Комп’ютерна криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – К.: Вища школа. – 2002. – 504с.
15. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М.А. Иванов. – М.:Кудиц-Образ. – 2001. – 368 с.
16. Ростовцев А.Г. Алгебраические основы криптографии / А.Г. Ростовцев. – СПб.: Мир и семья. – 2000. – 353 с.
17. Стіренко С.Г. Забезпечення безперервного відтворення потокового відео в однорангових мережах з використанням erasures кодів. / С.Г. Стіренко,

А.В. Габінет, Ю.В. Костенко // Вісник НТУУ "КПІ". Інформатика, управління та обчислювальна техніка: збірник наукових праць. – К.: "Век+". – 2015. – № 62. – С. 105–110.

18. Сэвидж Д.Э. Сложность вычислений / Д.Э. Сэвидж. – М.: Факториал. – 1998. – 368 с.

19. Фомичев В.М. Дискретная математика и криптология / В.М. Фомичев. – М.: Диалог-МИФИ. – 2003. – 379 с.

20. Boroujerdi N. Cloud Computing: Changing Cogitation about Computing / N. Boroujerdi, S. Nazem // IJCSI International Journal of Computer Science Issues. – Vol. 9. – Issue 4. – 2012. – №3. – PP. 169-180.

21. Kawamura S. A fast modular exponentiation algorithm / S. Kawamura, K. Takabayashi, A. Shimbo // IEEE Transaction on Information Theory. – Vol. 94. – № 6. – 2015. – P.2136-2142.

22. Широчин В.П. Вопросы проектирования средств защиты информации в компьютерных системах и сетях / В.П. Широчин, В.Е. Мухин, А.В. Кулик. – К.: ВЕК++. – 2000. – 111 с.

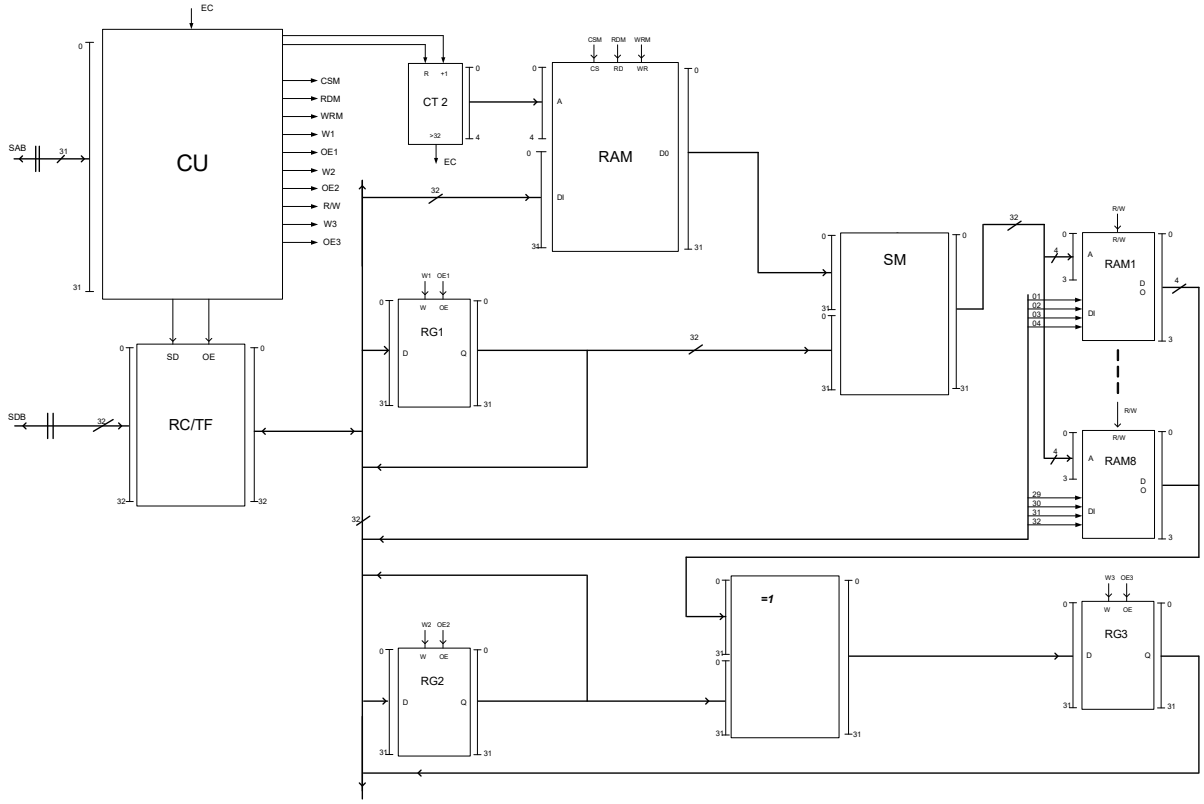
ДОДАТОК 1

Функціональна схема

ІАЛЦ.468243.004 Д1

Листів 1

2020



					ІАЛЦ.468243.004 Д1	
Змін.	*Арк.*	*№ докум.*	*Підпис*	*Дата*		
Розробив		*Іасешвілі Г.Н.*			*Процесор гомоморфного шифрування Схема електрична функціональна*	*Літ.* / *Аркуш* / *Аркушів*: 1 / 1
Перевір.		*Марковський О.П.*				
						КПІ ім. Ігоря Сікорського ФІОТ ІО-61
Н. контр.		*Симоненко В.П.*				
Затверд.		*Стіренко С.Г.*				

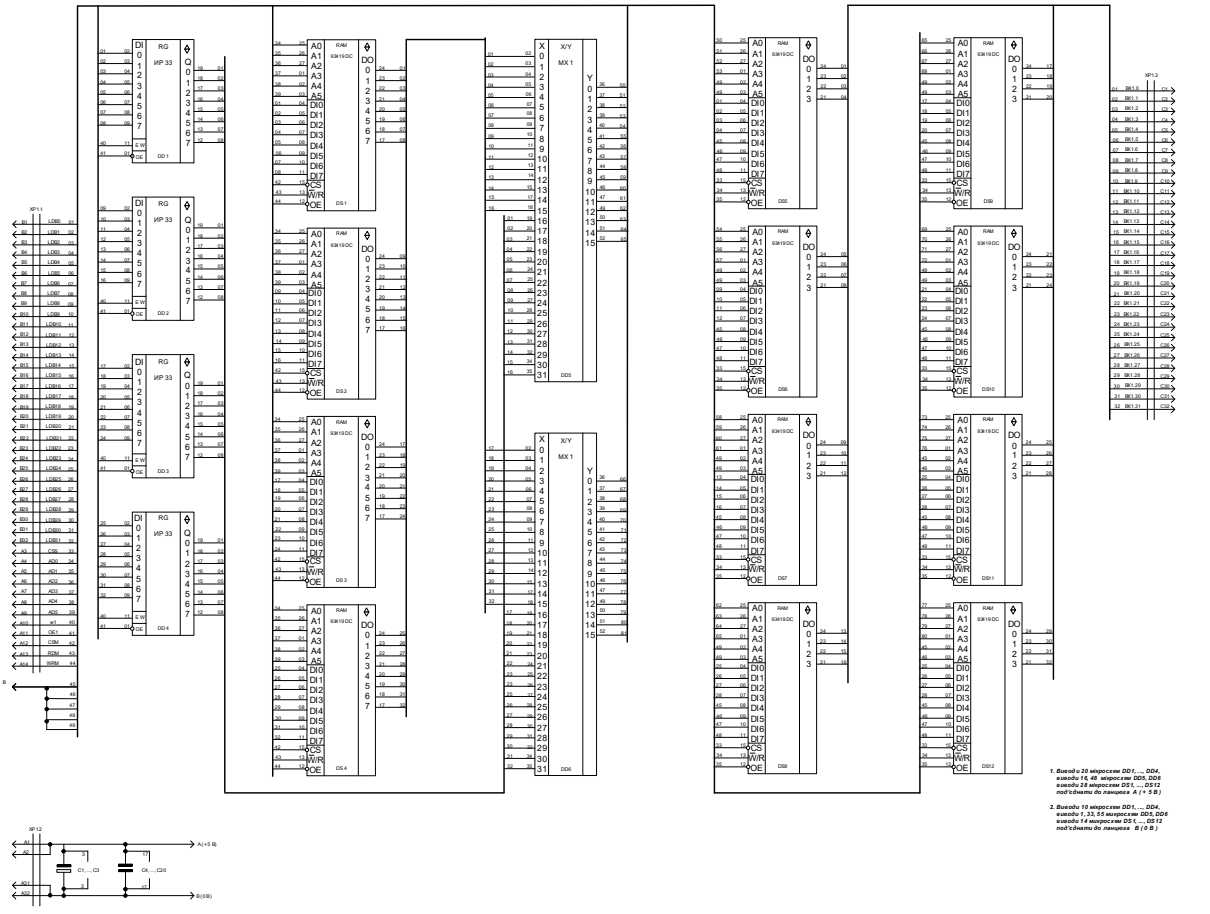
ДОДАТОК 2

Принципова схема

ІАЛЦ.468243.005 Д2

Листів 1

2020



Змін.	Арк.	№ докум.	Підпис	Дата	ІАЛЦ.468243.005 Д2		
Розробив		Іасешвілі Г.Н.			*Блок гомоморфного Шифрування Схема електрична принципова*	*Літ.*	*Аркуш* 1 / *Аркушів* 1
Перевір.		Марковський О.П.					
Н. контр.		Симоненко В.П.				КПІ ім. Ігоря Сікорського ФІОТ ІО-61	
Затверд.		Стіренко С.Г.					

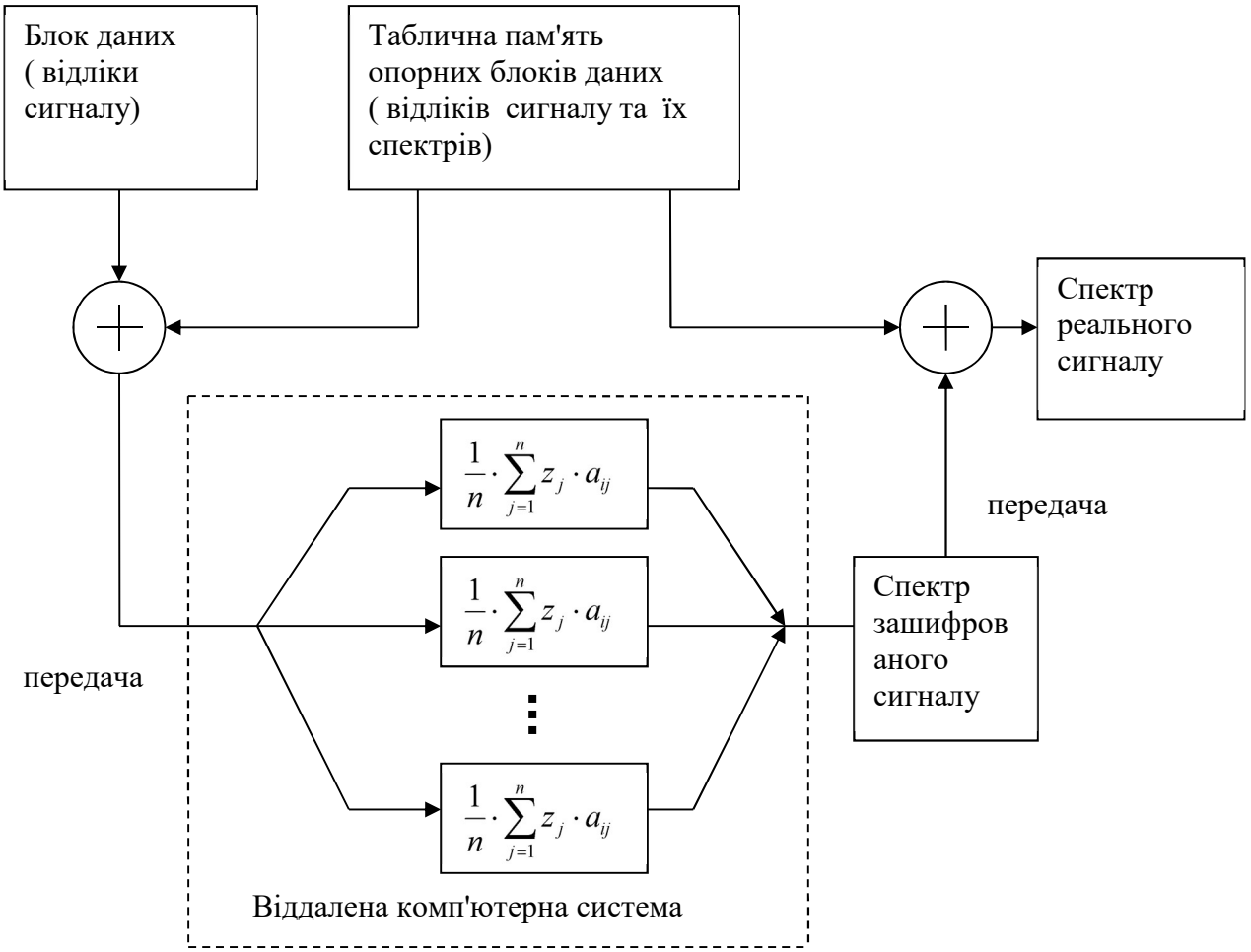
ДОДАТОК З

Структурна схема

ІАЛЦ.468243.006 ДЗ

Листів 1

2020



					ІАЛЦ.468243.006 Д3	
Змін.	Арк.	№ докум.	Підпис	Дата		
Розробив		Іасешвілі Г.Н.			*Процедура гомоморфного шифрування Схема алгоритма класу*	Літ. / Аркуш 1 / Аркушів 1
Перевір.		Марковський О.П.				
Н. контр.		Симоненко В.П.				КПІ ім. Ігоря Сікорського ФІОТ ІО-61
Затверд.		Стіренко С.Г.				